INFORMATION ASSURANCE

Legal, Regulatory, Policy and Organization Considerations

3rd Edition

17 September 1997

"We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."
[Joint Vision 2010]

INFORMATION ASSURANCE

Legal, Regulatory, Policy and Organizational Considerations

3rd Edition

17 SEPTEMBER 1997

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-6000

J-6A 00973-97
SEP 24 1997

To: Distribution List

Subject: Information Assurance(IA): Legal, Regulatory, Policy and Organizational Considerations

1. Information Superiority provides the foundation for the new joint operational concepts, outlined in Joint Vision 2010. Information Operations(IO) encompass the full range of offensive and defensive actions taken to ensure Information Superiority is established and maintained for the warfighter. Within IO lies the subset of IA, a process of critical defensive, layered-in-depth actions which guarantees our capability to collect, process and disseminate an uninterrupted flow of information. This study focuses on the Defense, Government and civil/commercial regulatory, policy and organizational considerations for national IA.

2. *Eligible Receiver-97*, and *Evident Surprise-97* are just two of the many recent exercises which have emphasized the difficulties we face in defending the DII(Defense Information Infrastructure) and the NII (National Information Infrastructure). Our ability to defend the network-centric NII and DII structures is dependent upon establishing cross-agency policy and procedures to coordinate effective defense, detection, and reaction IA capabilities.

3. This study is solely a research effort. Any judgments expressed or implied are those of the study group and should not be interpreted as official Department of Defense positions. By illuminating key IA concerns and serving as an apolitical source of information about IA, this document serves as a valuable tool in the creation IA policies and procedures. I wish to thank all contributors for their continuing efforts to support the accuracy and currency of this publication.

4. To save time and money, the Organizational and Reference Appendices found in Editions 1 and 2 will now be published only in even-numbered editions. We would appreciate user feedback regarding this product. If you have any questions or comments regarding this report, please contact COL Bob Gorrie, USA at 703-614-7812/Email gorrierg@js.pentagon.mil, or his lead action officer for this effort, CDR Nick Harris, USN at 703-614-5990/Email harrisbn@js.pentagon.mil.

Douglas D Buchholz

DOUGLAS D. BUCHHOLZ
Lieutenant General, USA
Director for Command, Control,
Communications and Computer
Systems

PREFACE

The emergence of Information Operations and its complex component of Information Assurance has been fueled by two things: the explosive proliferation of information-based technologies, and the necessity to reduce vulnerabilities throughout our global basing and information support networks. This report focuses on Information Assurance activities and initiatives undertaken since publication of the 2nd edition of this report in July 1996. Two themes became apparent during the research for this edition: 1) *convergence*: an evolving agreement on terminology and approaches, often engendered by critical operational requirements for collaborative efforts, and 2) accelerated *policy and doctrinal development* following a steadily increasing application of Information Operation practices and procedures in training, exercises and real world events. Together, these themes reflect a maturing of the DoD approach to IO. This maturing approach is based upon increased awareness and validation of emerging concepts.

In this report, the term *convergence* is viewed as the beginning of a process and shared corporate vision of the potentials available to the warfighter through *information superiority* — the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. This convergence reflects a broad agreement — and an essential teamed approach — on concepts, roles, and responsibilities relating to Information Operation activities. It has furthermore resulted in a clearer definition of terms, phrases, and doctrinal frameworks in the information environment.

The practical use and application of Information Operation activities by operating forces has validated concepts and fueled the parallel development of policy and doctrinal issues at strategic, operational, and tactical levels. Likewise, it has dramatically altered and accelerated the focus of legal, regulatory, and international aspects of Information Assurance and protection. This is not a unique situation in the evolution of warfare. Throughout history, exciting innovations and emergent requirements have routinely preceded and dramatically influenced the development of policy and doctrine.

The conceptual framework for the development and implementation of Information Assurance disciplines is embedded in *Joint Vision 2010.* This document provides the template and common direction for achieving unique capabilities and new levels of effectiveness in joint warfighting.

As viewed in Exhibit P-1, the organization of this report reflects a not-so-unfamiliar pattern of development in evolving strategies of warfare. *Operations* and practice (Section 2) necessitate *policy* decisions and *doctrine* development (Section 3). *Legal* (Section 4) aspects are reviewed, legislation is enacted, and *regulatory* (Section 5) guidelines, derived from statutes, are published. *International* (Section 6) community interests are measured and assessed, while the influence of rapidly emerging *technology* (Section 7) seeds new capability and serves as an enabling agent of change.

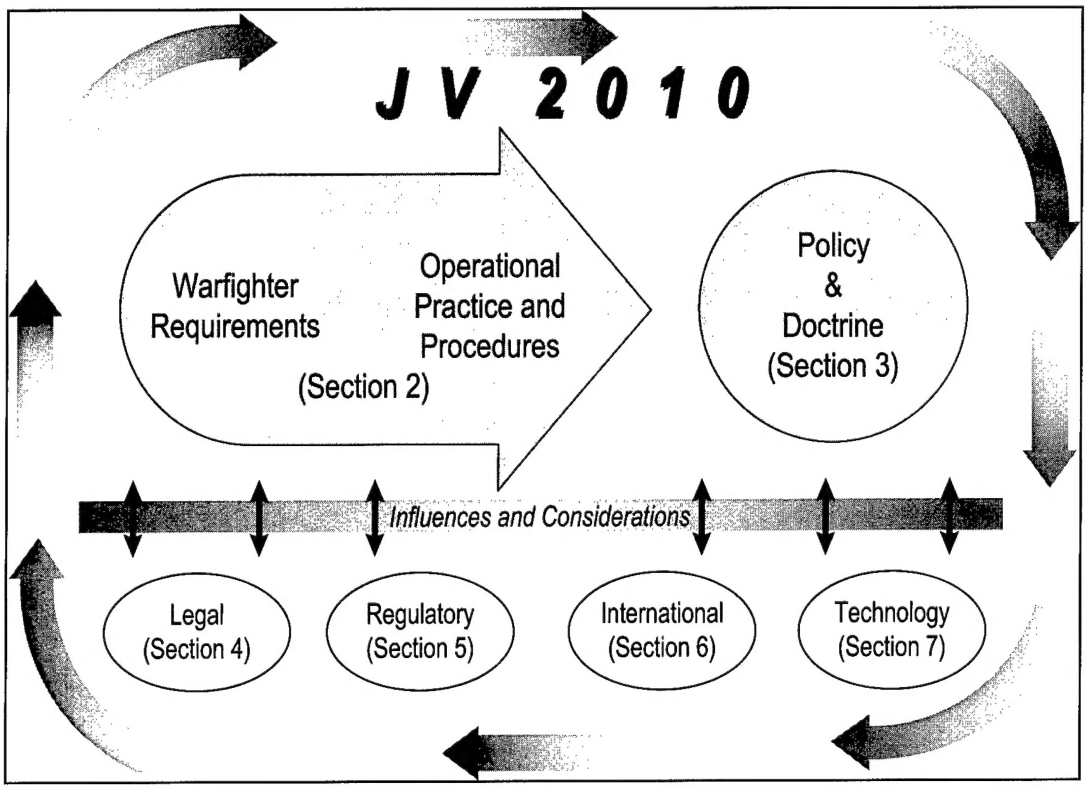


Exhibit P-1. Evolving IO Strategies

This 3rd edition builds on the information presented in previous editions. This edition is focused on a review of initiatives, issues, and events that have influenced policy formulation and doctrinal development of Information Assurance within DoD since publication of the 2nd edition. The change of title from *INFORMATION WARFARE* to *INFORMATION ASSURANCE* not only reflects a more precise description of content, but also is symbolic of the clarity and definition that Information Operations has achieved conceptually and organizationally since last year. It is representative of the teaming approach that policy, doctrine, and procedural development have attained in DoD.

Although considered an entire rewrite providing more granularity, this edition should not be viewed as a standalone document in some areas, such as the legal section. Though primary emphasis is on activities since July 1996, some background material from the 2nd edition has been carried over to this "yearbook" to enhance understanding. This edition does not include organizational updates and details as depicted in Appendix A of the 2nd edition. Readers are invited to refer to the Universal Resource Locators (URLs) listed for each organization in last year's edition for current information. Further information on organization-unique Information Assurance activities and points of contact may by provided in subsequent editions to this document.

Emphasis on the current status of law (Section 4) and regulations (Section 5) reflects the significant nature of these topics with regard to Information Assurance-related activities.

As in many other areas, there has been progress made on agreement of terminology. The report recognizes this fact and will address areas of divergence that remain. Key terms are defined in the body of the report for emphasis and to enhance comprehension of the issues discussed. See also Appendix C, Glossary.

The information contained in this document is current as of September 1, 1997.

This page intentionally left blank.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

LIST OF EXHIBITS

LIST OF EXHIBITS (Continued)

This page intentionally left blank.

SECTION 1

INTRODUCTION

This section describes the purpose and scope of the report and reviews relevant background, concepts, and terminology presently used by Department of Defense (DoD) and Government agencies in the information environment. Economic and information infrastructures are discussed to provide the reader with a sense of the magnitude, complexity, and interdependency of critical infrastructures on military operations and our economic security. Information assurance and protection issues are identified as a foundation for further emphasis on policy, legal, regulatory, international, and technical aspects in subsequent sections.

CONTENTS

1.1 PURPOSE

Joint Vision 2010 [1] embodies a concept of worldwide information superiority. This information superiority requires systems that are secure, dependable, and interoperable. As new technologies emerge and leading-edge C4I architectures are developed and fielded to provide warfighters total battlespace awareness, there is a growing urgency to ensure that the information, information systems, and information-based processes supporting those architectures are adequately protected. This report will assist the Joint Staff, in cooperation with other DoD elements, U.S. Government agencies, and industry representatives in formulating a comprehensive strategy to protect information, information systems, and information-based processes in support of *Joint Vision 2010.*

1.2 SCOPE

This report focuses on Information Assurance activities and initiatives that are the most relevant to DoD missions. Within this context, Infrastructure Protection is addressed as it relates to critical information system dependencies that support vital DoD missions across the full range of military operations.

This is the 3rd edition in a continuing series of reports that review initiatives, issues, and events influencing policy formulation and doctrinal development of Information Assurance during the preceding year. Although the report has been completely rewritten, it builds on the work of previous editions and, therefore, should not be viewed as a standalone document. Though the report emphasizes activities that have occurred since July 1996, preceding background material is provided for clarity and understanding.

---

[1] Department of Defense (DoD), Chairman of the Joint Chiefs of Staff (CJCS), *Joint Vision 2010* (undated).

As seen today, the powerful nature of Information Warfare and its complex component of Information Assurance reflects a dynamic interplay and parallel evolution of practice and theory, operations and doctrine, legal and regulatory implications, and the undeniable influence of rapidly emerging information-based capabilities available to the joint warfighter. The organization of this report reflects this not-so-unfamiliar pattern of development in evolving strategies of warfare: operations, policy, legal aspects, and the exploitation of information and integration of information system technologies.

1.3 BACKGROUND

This section introduces current Office of Secretary of Defense (OSD) and Joint Staff high-level frameworks for Information Operations. These frameworks provide a baseline for the continuing evolution of Information Operations and Information Assurance and are intended to enhance the reader's understanding of the remaining sections of this report.

1.3.1 Information Operations

This report and previous editions of the report provide an annual snapshot of the state of information warfare/information operations within the Federal government, DoD, and other organizations. The following thoughts capture the essence of DoD Information Operations (IO) and Information Assurance (IA) activities reflected in these three reports:

1995 — Identifying and framing the issues

1996 — Seeking consensus and alternative solutions

1997 — Convergence.

These are statements reflecting the general state-of-affairs within DoD. Admittedly, some organizations and echelons within DoD have long been *fully engaged* in Information Operations and Assurance activities. One could also argue that the enterprise is still grappling with issues and alternative solutions. The 1st edition of this report sought to identify the stakeholders, the issues, and approaches and models for addressing the issues. The 2nd edition reflected heightened awareness and activity in IO/IA, but there was no broad agreement on priorities, approaches, and solutions. The 3rd edition reflects broader agreement on concepts, doctrine and policy, and roles and responsibilities. Even the title of this 3rd edition—Information Assurance—reflects the changing terminology. *Convergence* indicates the beginning of a process, rather than an end state. Much of the progress can be attributed to the work of professionals across the breadth and depth of DoD, in cooperation with other agencies of the Federal government and with industry. Two seminal documents, discussed in the following sections, reflect, and to some extent have contributed to, this embryonic convergence of ideas and actions.

1.3.2 Joint Vision 2010 and a Joint IO Framework

The first seminal document, *Joint Vision 2010*, was issued by the Chairman of the Joint Chiefs of Staff in July 1996. The vision captured in this document emphasizes information superiority—the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. This concept focuses on the data and information processing capabilities required by the joint warfighter and suggests prioritizing and protecting information based upon warfighter needs.

Joint Vision 2010 (JV2010) is a conceptual framework of common direction for the Services in developing unique warfighting capabilities. *JV2010* seeks to achieve Full Spectrum Dominance of an adversary through four reinforcing emerging operational concepts — Dominant Maneuver, Precision Engagement, Full-Dimensional Protection, and Focused Logistics. These four operational concepts are enabled by Information Superiority which is based, in part, upon Technological Innovations. Exhibit 1-3-1 depicts the *JV2010* concept.

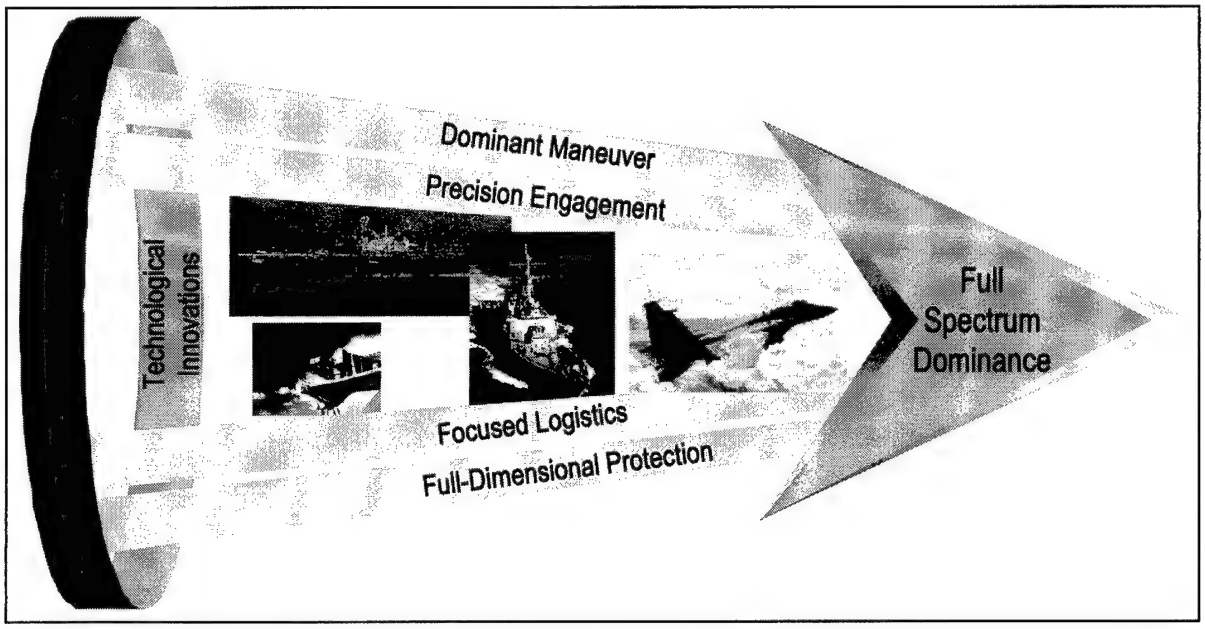


Exhibit 1-3-1. Joint Vision 2010

JV2010 also anticipates accelerated operational tempos, even for higher level commanders, creating "a more stressful, faster moving decision environment. Real-time information will likely drive parallel, not sequential, planning and real-time, not prearranged, decisionmaking." This vision of future operations and its four operational concepts build upon and require information superiority; it assumes a real-time, unrestricted flow of information. *JV2010* cites the protection of the ability to conduct information operations as one of the biggest challenges in the future. This protection will require traditional (e.g., physical security and encryption) and nontraditional (e.g., antivirus protection and innovative secure data transmission) techniques.

JV2010 preceded DoD Directive S-3600.1, *Information Operations*, [2] which is discussed in Section 1.3.3, and, therefore, reflects the information warfare terminology (offensive and defensive) of the earlier version of the Directive. This shortcoming does little to weaken the pivotal message that successful joint operations in the future will rely upon Information Superiority and effective defensive information warfare operations/information assurance.

The Joint Staff has developed a doctrinal framework that is important for the reader to understand. Exhibit 1-3-2 depicts this framework and is based largely upon definitions found in the Chairman of the Joint Chiefs of Staff Instruction 6510.01B, *Defensive Information Operations*, [3] and the second draft of Joint Publication 3-13, *Joint Doctrine for Information Operations*. [4]

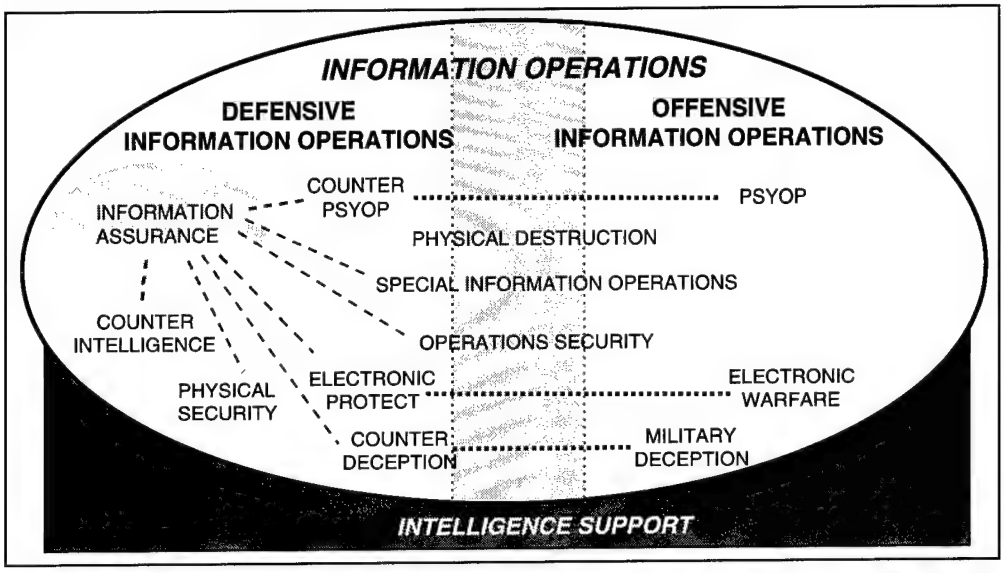


Exhibit 1-3-2. Joint IO Framework

Exhibit 1-3-2 depicts Defensive and Offensive IO as subsets of IO with shading between the two to indicate the required integration and coordination. The dotted lines, e.g., between Counter Psychological Operations (PSYOP) and PSYOP, indicate relationships where further integration and coordination is necessary. The dashed lines from IA to the other disciplines reflect that assurance results from the coordinated or layered implementation of all of these disciplines. In day-to-day peacetime operations, Counterintelligence, Physical Security, and Operations Security tend to be paramount. During crisis and war, the other disciplines take on increasing importance. Exhibit 1-3-3 provides narrative joint definitions for Defensive and Offensive IO.

---

[2] DoD, Department of Defense Directive (DoDD) S-3600.1, *Information Operations (IO) (U)* (9 December 1996).
[3] DoD, CJCS, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01B, *Defensive Information Operations* (22 August 1997).
[4] DoD, The Joint Staff, Joint Publication 3-13, *Joint Doctrine for Information Operations, Second Draft* (2 July 1997).

Defensive Information Operations: The defensive IO process integrates and coordinates polices and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations. Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes.

Offensive Information Operations: The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Exhibit 1-3-3. Joint Definitions (Joint Pub 3-13, draft)

The primary focus of previous editions — and the title of this report — has been on Information Assurance (in the 1st and 2nd editions, the *term d'art* was Defensive Information Warfare). However, it has always proven difficult to limit discussions fully to IA, nor would it necessarily be beneficial to do so. Therefore, as appropriate, the terms Information Operations and Defensive Information Operations are used. IA is used when the focus of the discussion is principally on the protection of information and information systems. Defensive Information Operations is used when the focus is on a broader range of issues and, in particular, when the discussion addresses joint warfighting concepts.

In recognition of the dependency of joint warfighting on non-DoD owned and operated systems and infrastructures, the Joint Staff has defined or adopted terms which help describe the information environment. A few of these key terms, defined in CJCSI 6510.01B and Joint Pub 3-13, are provided in Exhibit 1-3-4.

Critical Infrastructures: Certain national infrastructure so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical, power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Information-based Processes: Processes that collect, analyze and disseminate information using any medium or form. These processes may be standalone processes or subprocesses which, taken together, comprise a larger system or systems of processes.

Global Information Infrastructure (GII): Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services.

National Information Infrastructure (NII): The NII is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the Government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks.

Exhibit 1-3-4. Defining the Environment

1.3.3 DoD Directive S-3600.1, *Information Operations*

On 9 December 1996, Deputy Secretary of Defense White signed out DoD Directive S-3600.1, *Information Operations*, updating DoD policy on Information Operations (IO) and Information Warfare (IW) and superseding DoD Directive TS-3600.1, *Information Warfare.* [5] The revised directive reflected the conceptual evolution as well as a general convergence in understanding and approach to IO within DoD. This concept of IO is depicted in Exhibit 1-3-5, a Joint Staff graphic.

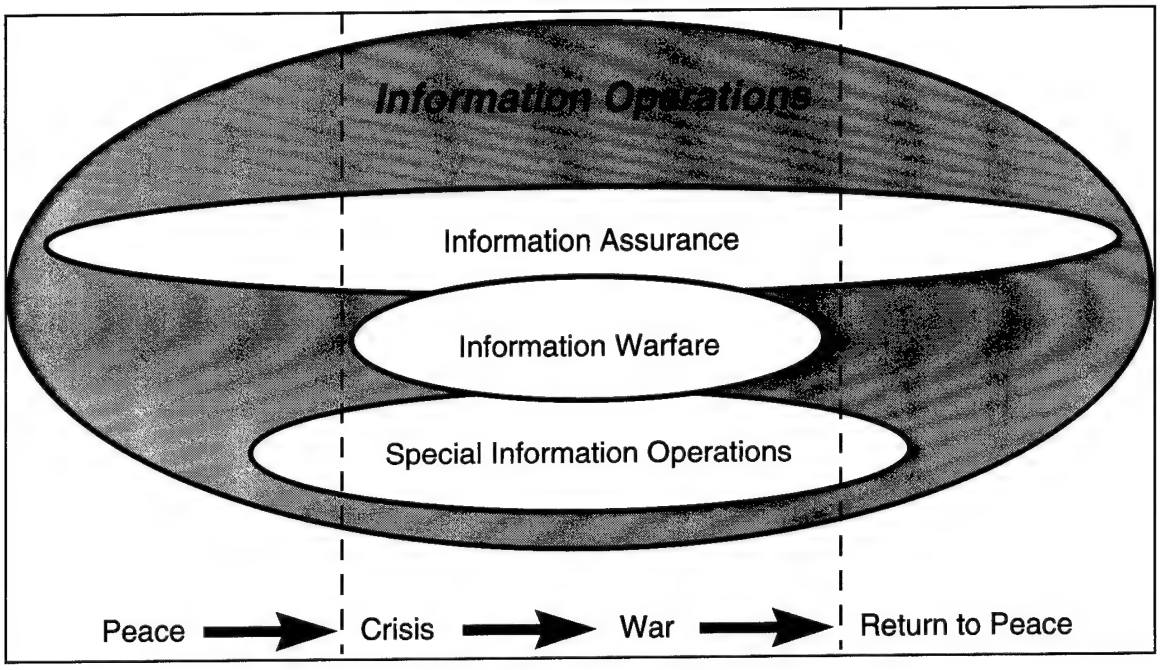


Exhibit 1-3-5. Information Operations

The revised directive embraced IO, a term already in use in some Service doctrine, as an umbrella term inclusive of the universe of defensive and offensive information activities within the information environment. The concept also distinctly separated peacetime information operations from information warfare activities during crisis and war. Information Assurance, encompassing what was previously peacetime defensive information warfare (IW-D) activities, would facilitate coordination with those outside of DoD, such as the civil agencies of the Federal government, industry and the public. At times, it was difficult to address defensive information *warfare* issues with those for whom *warfare* was not a part of the mission or culture. The adoption of IA reflects the recognition that IO are larger than DoD and that successful IO, particularly IA, depend upon the integration and cooperation of DoD, Federal, industry, and public efforts. At the same time, the term "IA" encompasses a concept larger in scope than the classic information security and information systems security (INFOSEC), which have long been largely associated with the protection of classified national security information and information systems.

---

[5] DoD, DoDD TS-3600.1, *Information Warfare (U)* (21 December 1992).

The terms defined in DoD Directive S-3600.1 provide a framework for IO. Throughout this report, the reader will find references to DoD initiatives. These initiatives encourage a culture change embracing the IO framework and are intended to ensure that the implications of the new framework are fully understood and addressed. To obtain a clear understanding of the issues, the reader must first understand the terms used. Exhibit 1-3-6 provides an extract of the terms defined in the Directive.

Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Information: Facts, data, or instructions in any medium or form.

Information Assurance: Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Environment: The aggregate of individuals, organizations, or systems that collect, process or disseminate information, also included is the information itself.

Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare: IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Special Information Operations (SIO): IO that by their sensitive nature, due to their potential effect of impact, security requirements, or risk to the national security of the United States, require a special review and approval process.

Exhibit 1-3-6. DoD Directive S-3600.1 Definitions

1.4 INFRASTRUCTURES

This section briefly discusses the nature and interdependencies of functional activities and infrastructures. Certain of these infrastructures have been designated as critical — telecommunications, electric power, gas and oil production, storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government services. [6] The section touches on some of the legal, regulatory, policy, international, and technical aspects (which are discussed later in the report) to give the reader a sense of the complex interrelationships of these activities and infrastructures.

1.4.1 Nature of Infrastructures

The production and delivery of goods and services directly affect the national and economic security of the United States and directly influence the readiness of the military forces. The delivery of these goods and services depends on the complex interactions of various functional activities, industries, commodities, and political, economic, and social conditions.

[6] The President, Executive Order 13010, *Critical Infrastructure Protection* (15 July 1996).

Consider, for example, the functional activity of deploying a military force from the United States to deal with a regional crisis. This deployment requires moving individual units to ports of embarkation, transporting those units to the region of interest, and employing the force to deal with the crisis. If the deployment involves a sizable force, these activities depend, in turn, on the use of the nation's transportation infrastructure. Coordinating the activities depends on an effective telecommunications infrastructure. Both the transportation and telecommunications infrastructures depend on the availability of electrical power, which depends on the availability of sufficient energy sources. Coordinating transportation activities and providing electrical power also depend on an effective telecommunications infrastructure.

In general, U.S. infrastructures are extremely reliable and available because they have been designed to respond to disruptions, particularly those caused by natural phenomena. Redundancy and diverse routing are two design techniques used to improve reliability and availability. However, companies operating these infrastructures are relying more and more on information technology to centralize control of their operations and to provide service to their customers. This centralization and the increased reliance on broadly networked information systems increase the vulnerabilities of the infrastructure and the likelihood of disruptions or malevolent attacks.

1.4.2 Infrastructure Protection and Assurance

Infrastructure protection, or protecting the infrastructures against physical and electronic attacks, will be complicated. These infrastructures are provided mostly (and in some cases exclusively) by the private sector; are regulated in part by Federal, state, and local governments; and are significantly influenced by varied market forces. Commercial services from the national information infrastructure provide most of the telecommunications portion of the Defense Information Infrastructure (DII). These services are regulated by Federal and state agencies. Local government agencies regulate the cable television portion of the information infrastructure. Power generation and distribution are provided by very diverse activities — the Federal government, public utilities, cooperatives, and private companies. Interstate telecommunications are regulated by the Federal Communications Commission; intrastate telecommunications, by the state public utilities commissions. Interstate power distribution is regulated by the Federal Energy Regulatory Commission; intrastate power generation and distribution, by the state public utilities commissions.

To add to this confusion, the *Telecommunications Act of 1996* [7] decreases regulation of the industry and encourages the eventual entry of long-distance telecommunications, local telecommunications, and cable television service providers into each other's markets. This deregulation will increase competition and reduce the cost of services. Power industry utilities, for example, are very interested in using their extensive rights-of-way to homes and businesses to leverage their entry into the telecommunications market. Utilities are already testing these concepts, introducing several new players into the telecommunications infrastructure.

---

[7] United States, *Telecommunications Act of 1996,* Pub. Law No. 104-104, 100 Stat. 56 (1996). Full text available on U.S. Federal Communications Commission (FCC) site on Internet at http://www.fcc.gov/telecom.html

The concept of *infrastructure assurance* is also important to understand. Infrastructure assurance differs from infrastructure protection in subtle, yet important, ways. *Infrastructure protection* means protection of an infrastructure from physical or electronic attack. *Infrastructure assurance* includes those actions needed to ensure readiness, reliability, and continuity of an infrastructure. These actions make the infrastructure less vulnerable to disruptions or attack; restrict damage in the event of a disruption or attack; and enable the infrastructure to be readily reconstituted to reestablish vital capabilities. [8]

Several factors influence infrastructure assurance. The most significant of these factors is the market. Competitors providing services within an infrastructure will invest to ensure robust and reliable service, but only to the extent necessary to retain or grow market share. Regulation of service providers within an infrastructure is generally undertaken only to ensure safety and availability of service or to control the price of the service. Potential liability is another factor which influences a service provider to ensure robust and reliable service. An acknowledgment of infrastructure vulnerabilities, however, increases the potential liability of a service provider; the service provider is less likely to acknowledge or share information about those vulnerabilities.

The interaction of these market, regulatory, and potential liability forces in an environment of rapid change (such as the telecommunications market) cannot be predicted, let alone fully understood. It is important, however, to recognize the potential influence of these forces in determining infrastructure protection strategies for the near future.

There are many legislative, regulatory, policy, and technical questions still to be answered regarding infrastructure protection and assurance: What is the legitimate role of DoD or the Federal government in ensuring the availability of these infrastructures to support critical functions? Who should pay for improvements needed to ensure availability? Who should guide the needed efforts? How should critical portions of the infrastructures be protected? What are service implications of added protection? Because of a growing understanding of infrastructure dependencies, these and many similar questions are now being asked by a growing body of stakeholders. While this report does not answer the questions, it does examine some of the complexities of the problem, in the hope of facilitating among the stakeholders discussions that will lead to solutions.

1.4.3 Infrastructure Assurance and Information Assurance

Infrastructure assurance and information assurance are related; information assurance leads to infrastructure assurance. Infrastructures are operated and controlled through information and information technology. Information assurance of these information components of infrastructures is a necessary, but not sufficient, condition of infrastructure assurance.

---

[8] DoD, Office of the Undersecretary of Defense for Policy (OUSD(P)), Critical Infrastructure Protection Working Group (CIPWG), *Options for Protecting the Critical National Infrastructures* (6 February 1996)

SUMMARY

- This edition recognizes a convergence and broader agreement on concepts, doctrine, roles, and responsibilities relating to Information Operation activities.
- Convergence has required, and generally resulted in, clearer definition of terms, phrases, and doctrinal frameworks in the information environment.
- *Joint Vision 2010* provides evolutionary challenges for the warfighter by identifying the focal nature of information flow and protection in combat capability.
- Military operations and economic security depend on the availability of complex industries and information systems — critical infrastructures.
- Market forces, deregulation, and the interdependent nature of critical infrastructure systems will challenge the essential development of critical asset protection strategies.

SECTION 2

DEFENSIVE INFORMATION OPERATIONS

The purpose of this section is to introduce some basic defensive information operations concepts with emphasis on information assurance. This section describes some of the current operations practices which will influence the parallel development of policies and doctrine. This section also provides the operational context for the discussions of the policy and doctrine, legal, regulatory, and technology aspects of information assurance in the subsequent sections. This section emphasizes the information assurance aspects of defensive information operations. It does not address physical security, operations security, counter-deception, counter-psychological operations, counter-intelligence, electronic protect, or special information operations.

CONTENTS

2.1 EVOLVING DEFENSIVE INFORMATION OPERATIONS STRATEGY

The policy and doctrine for command and control warfare [9] provide the foundation for a defensive information operations strategy, but are limited in application to the broader issues associated with protecting and defending the Defense and national information infrastructures. Consequently, the defensive information operations strategy has been evolving over the past few years. This evolution is based on information systems security practices, lessons learned from Desert Storm/Shield, emerging concepts on defensive information warfare, partial implementation of those concepts, a series of operational exercises and real-world incidents. This section of the report will briefly review some of the pertinent policies, discuss some of the emerging concepts, and summarize the evolving defensive information operations strategy.

The previous editions of this report and Section 3 of this report discuss the details of pertinent policy and doctrine. Some of the key policies bearing on the evolution of the defensive information operations strategy include the following:

- (U) "Information, information systems, and information-based processes (such as C2, communications, weapon systems, etc.) used by U.S. military forces will be protected relative to the value of the information they contain and the risks associated with its compromise, or loss of access." [10]

---

[9] DoD, Joint Staff, Publication 3-13.1 *Joint Doctrine for Command and Control Warfare (C2W)* (7 February 1996).
[10] DoD, CJCS, Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01 (SECRET), *Joint Information Warfare Policy* (U) (2 January 1996).

- (U) "Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure ....Components shall create realistic IO environments for planning, training, and acquisition purposes to include models and simulations." [11]
- (U) "Command and control of forces shall be planned and exercised to ensure critical information is adequately protected from adversary IW effects and U.S. forces can operate successfully in degraded information and communications environments." [12]
- (U) "The combatant commanders will incorporate offensive and defensive IW concepts into deliberate ... and crisis actions plans ...." [13]
- (U) "All DoD elements will adopt a risk management approach to protection of their information, information systems, and information-based processes based on potential vulnerability to IW." [14]

As a part of the policy formulation, the Joint Staff developed a model for defensive information operations implementation process. The model is shown in Exhibit 2-1-1.

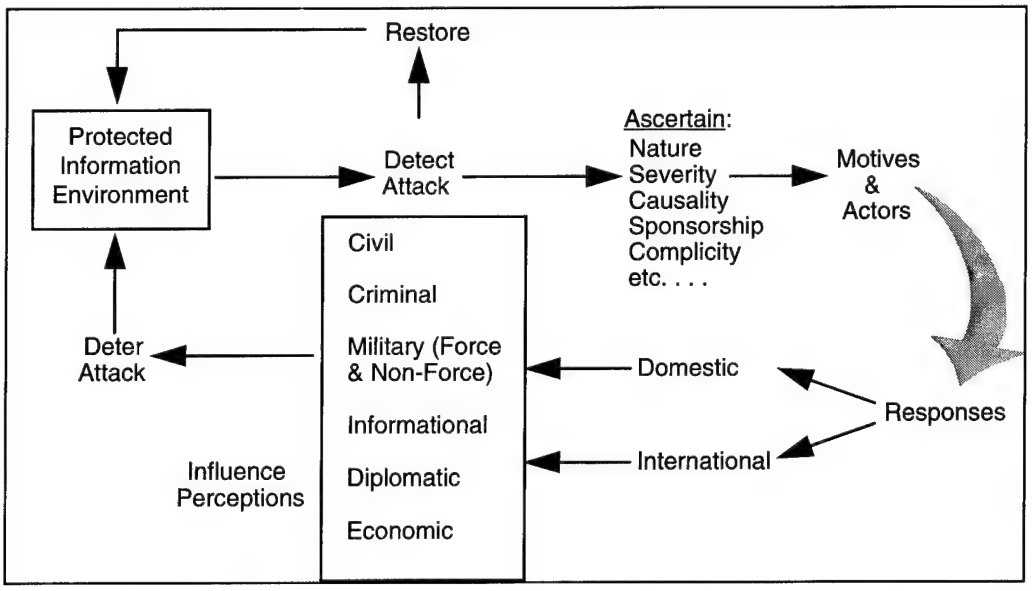


Exhibit 2-1-1. Defensive Information Operations Implementation Process [15]

The following discussion of the model is based on the source policy document, the recommendations of the Defense Science Board Task Force on Information Warfare - Defense (discussed in more detail in Section 3.2.1), and evolving concepts based on exercise and operational experience. A key point not reflected in the Implementation Model is that the procedure must be a distributed process. The basic functions of monitoring, detection, damage

[11] DoDD S-3600.1, *Information Operations (IO)* (U) (9 December 1996).
[12] Ibid.
[13] CJCSI 3210.01, *Joint Information Warfare Policy.*
[14] Ibid.
[15] CJCSI 6510.01B, *Defensive Information Operations* (22 August 1997).

control, and restoration must begin at the lowest possible operating level. Reports of the activity must be passed to regional and higher-level organizations to establish patterns of activity and to request assistance as needed in damage control and restoration.

Protected Information Environment. A key first step in the model is to identify the critical functions and information that must be protected, how they should be protected, and to what extent they should be protected. As suggested in policy, they should be protected relative to the value of the information they contain and the risks associated with compromise, or loss of access.

This first step led to a need to establish a protected information environment. The degree of protection required should be based on documented policies and on basic and fundamental risk management techniques. This protection should be employed in **layers** in order to defeat nuisance attacks with minimum resources and permit early warning of more significant attacks.

For example, Professor David Alberts of the National Defense University proposes a "defense-in-depth" strategy. [16] This strategy involves a series of successively stronger defensive barriers that work together to decompose the spectrum of threats into manageable pieces. Under normal conditions, information availability is the first priority; under high threat conditions, security is the first priority.

Protection is based on the principles of good security — administrative, personnel, physical, and information security. It might include physically isolating information, access control, authentication of personnel performing critical functions or accessing information, encryption of information, employment of intrusion detection capabilities, and similar precautions. As time and resources permit, the information infrastructure supporting the critical functions should be designed for utility, resiliency, repairability, and security.

It is important to verify through independent vulnerability assessments that the design is being followed, that protective measures are being implemented where appropriate and as dictated by policy, and that operational and security postures are as reported. ("Red Teaming" is the emerging term to describe these assessments.) Procedures to implement the policy should include formal approval for connection to sensitive networks and certification and accreditation of certain systems, networks, and network connections.

An equally important aspect of a protected information environment is making users and operators of the environment aware of the threats to and potential vulnerabilities of the environment. For example, users should be taught to recognize possible malicious disruptions of the environment and report such incidents. Systems administrators should be trained and certified to ensure that the "first line of defense" is prepared to deal with potential attacks against the protected environment. Professionalization of appropriate military and civilian employees increases the capabilities to meet the threat. It is also essential to involve public affairs and command information personnel in defending against perception management by the adversary.

---

[16] David Alberts, *Defensive Information Warfare* (Institute for National Strategic Studies, National Defense University: Washington, DC 1996).

Detect Attack. To detect attacks on the protected information environment requires intelligence support and use of the proper procedures and tools. The need to provide intelligence support to infrastructure assurance cannot be overemphasized. This support must include accurate threat assessments, indications and warning of potential attacks, and timely current intelligence support in the event of an actual attack. DoD and national-level intelligence organizations; law enforcement agencies at the local, state, national and international levels; and private-sector organizations capable of adding depth to the intelligence estimates should all cooperate in providing this support. Subsequent sections of this report discuss in more detail the relationship of the defensive information operations community with the intelligence community (Section 2.3.6) and the law enforcement community (Section 2.3.7).

Appropriate networks and systems must be monitored in order to detect infrastructure disruptions, intrusions, and attacks. Current intrusion detection and computer audit data reduction techniques (Section 7) provide a rudimentary capability. All intrusions and related incidents should eventually be reported and correlated to establish "normal" operating patterns and identify "abnormal" activity to aid in developing indications and warning. DoD is in the process of developing and implementing reporting thresholds, procedures, and mechanisms. Integrating this cyber-war operational information into the intelligence and operations picture of the battlefield is another challenge only now being addressed.

Providing an effective monitoring, detection, reporting, and warning capability involving other government organizations and the private sector will require policy initiatives, some legal and regulatory clarification, and an ambitious research and development program. Aspects of these issues are discussed in Section 3 (Policy and Doctrine), Section 4 (Legal), Section 5 (Regulatory), and Section 7 (Technology).

Restore. There are a variety of approaches and means to restoring information, information systems, and information-based processes. An emergency reaction capability is necessary to control the damage that results from an attack and to restore the protected information environment. The Combatant Commands, the Services, and the Defense Information Systems Agency have a computer emergency reaction capability but a limited capability to minimize damage and restore the protected information environment. These functions require extensive involvement of network and systems managers. Little research has been devoted to developing the basic procedures necessary to contain "battle" damage, let alone to the tools which might provide some automated form of damage control. Knowledgeable personnel, standby services contracts, and the like are necessary to repair the damage.

Ascertain Motives and Actors. To determine the impact of an attack on critical functions and information and the appropriate manner in which to respond to an attack, a capability to assess attacks is needed. Such an assessment involves determining the nature and severity of the attack and its sponsorship, and possible complicity by an insider in perpetrating the attack. It will require the participation of intelligence and law enforcement organizations, correlation of vast amounts of seemingly trivial information, and a broad perspective of the battlefield situation.

Responses. Based on the intent of the perpetrators and other circumstances, response to the attack might include prosecution, diplomatic efforts, perception management, or even the use of military force.

Deter Attack. A desired outcome of the Defensive IO Implementation Process is deterrence of future attacks.

One of the challenges in implementing the model has been the lack of adequate alerting mechanisms to heighten awareness and preparedness as the information threat changes. In addition, the defensive information operations community should probably implement procedures for responding to increasing threat conditions. Such procedures might include minimizing the traffic on the networks, restricting personnel access to operational facilities, disconnecting certain systems from networks that are likely targets, and possibly implementing wartime modes of operation. Further examples are discussed in Section 2.3.2 (Information Alert Conditions).

Another challenge has been the lack of adequately defined indications. This lack severely limits our ability to develop strategic warnings about growing offensive information operations capabilities. An effort is currently under way in the Joint Staff J2 to define these indications and warnings.

Finally, an organizational and decision support (command and control) structure is required to manage implementation of the model.

A variant on the aforementioned model has emerged based on the experience of U.S. Atlantic Command (USACOM). The defensive information operations model depicted in Exhibit 2-1-2 reflects the operations and exercise experience of the Command and is presented as a complementary view of the evolving strategy to encourage discussion and experimentation.

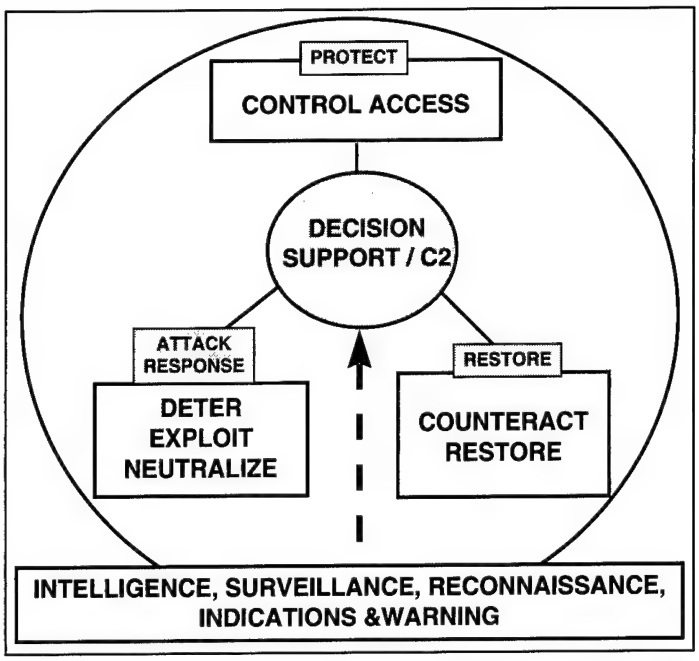


Exhibit 2-1-2. USACOM Defensive Information Operations Model

The USACOM model consists of three centrally controlled defensive information operations functions: protect, attack, and restore. Indications and warning, intelligence, surveillance, and reconnaissance support these three functions. The **protect** function controls adversary access to the friendly protected information environment. It consists of active and passive measures and incorporates the protect, monitor, detect, and reporting functions of the earlier model. The **attack response** function deters adversary attack, neutralizes the effects of such an attack, and exploits such an attack for friendly purposes. It consists of both preemptive and reactive measures and includes the functions of deter and respond. The **restore** function counteracts the effects of the attack and restores the protected information environment. It consists of proactive and reactive measures and includes the restore functions from the earlier model (Exhibit 2-1-1). The decision support (command and control) function controls the defensive information operations based on input from the indications and warning, intelligence, surveillance, and reconnaissance functions.

Exhibit 2-1-3 shows how the USACOM model can be used. The friendly protected information environment contains priority elements. These elements are critical to accomplishing mission objectives. In some cases, these elements are connected to the global information environment. The elements which make up the protected information environment will vary based on time, circumstances, and military objectives. The adversary information environment depicts key decisionmakers as the focus of friendly efforts. World opinion and 3rd parties are avenues of influence and action for both friendly and adversary parties. The strategy is to employ protect, attack response, and restore capabilities to achieve assigned missions and objectives.

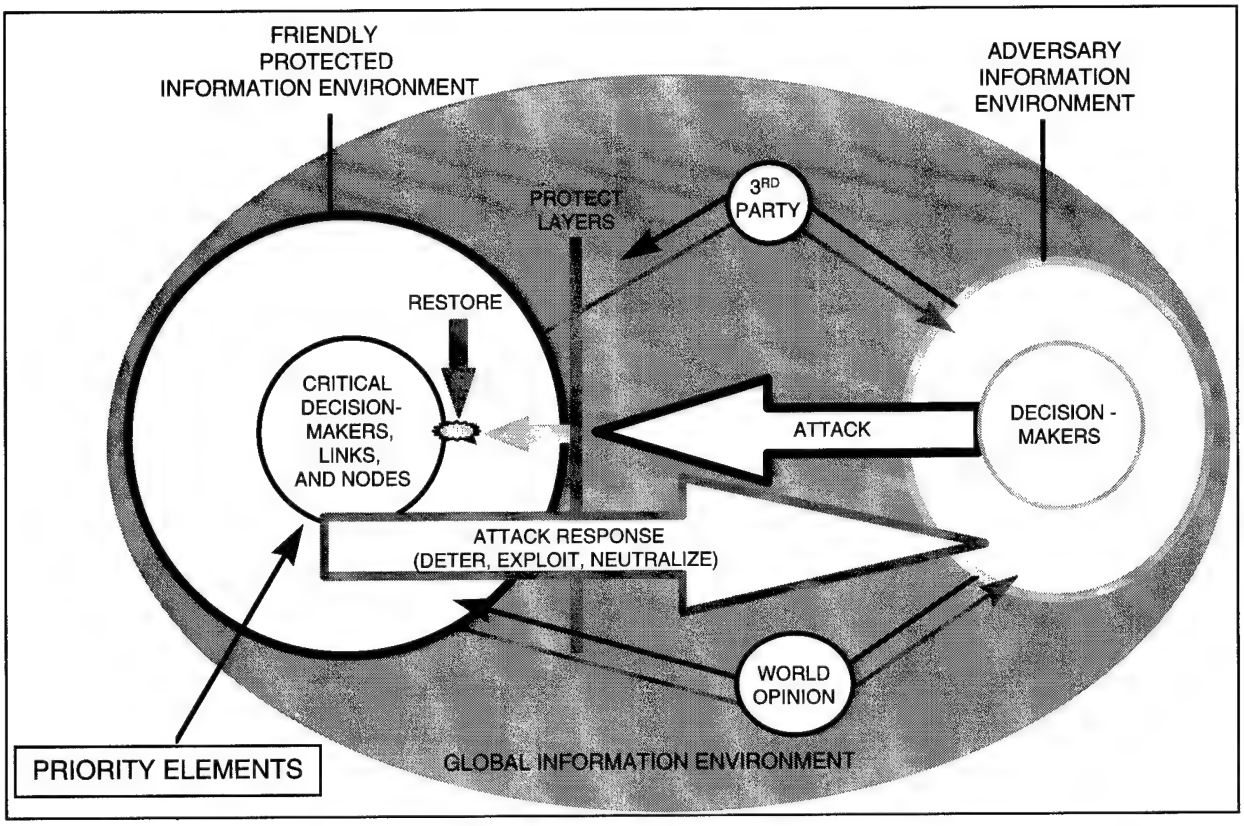


Exhibit 2-1-3. USACOM Defensive Information Operations Environment

The USACOM model and its implementation suggest a framework for a defensive information operations strategy as shown in Exhibit 2-1-4.

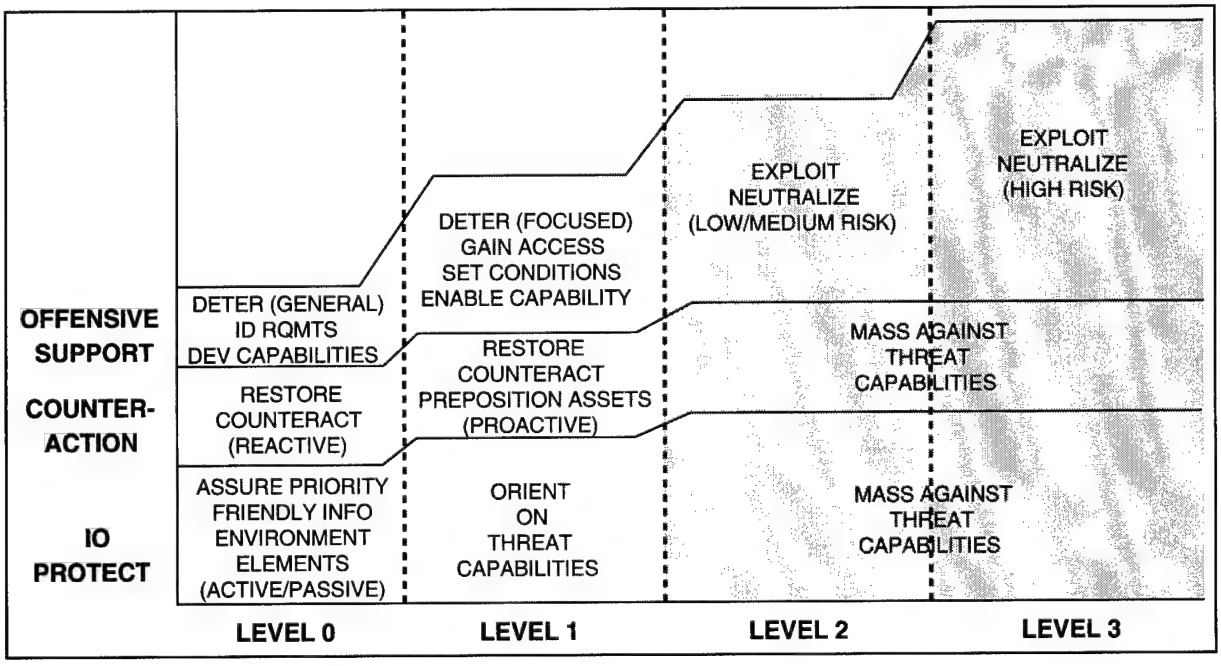


Exhibit 2-1-4. USACOM Defensive Information Operations Strategy

The elements of the USACOM strategy are contained within the framework. The functions of the model are shown on the left. The levels shown across the bottom indicate varying levels of operating conditions. The numbering system highlights the uniqueness of level 0 — an ongoing, continuous, and routine program of organizational defensive measures without regard to any specific threat. Each of the levels will eventually be described in terms of beginning conditions, task and purpose, priority of effort for each of the three functions of the model, responsibilities, command and control and coordination required, and ending conditions. These specific details, as well as the transition criteria for moving among levels, are under development. One of the transition criteria, for example, might be the information alert condition, examples of which are shown in Section 2.3.2 below. The term "level" is used rather than "phase" to describe operating conditions and to emphasize the fact that it is not necessary to step through each successive level. For example, a movement from level 0 to level 4 is possible within this framework.

2.2 FUNCTIONS AND RESPONSIBILITIES

To be effective, the evolving strategy in day-to-day operations must be implemented within the context of the traditional functions of the DoD components and the currently defined defensive information operations responsibilities.

Exhibit 2-2-1 summarizes some of these key functions and responsibilities. The exhibit shows the range of functions and division of labor to give the reader a sense of the difficulty in coordinating these functions in the current, information-intense, highly inter-networked operating environment. The functions and responsibilities are based on several policy directives. [17]

[17] (1) DoD, DoDD 5100.1 *Functions of the Department of Defense and Its Major Components* (25 September 1987).
(2) DoD, CJCSI 3210.01 (SECRET), *Joint Information Warfare Policy* (U) (2 January 1996).
(3) DoD, DoDD S-3600.1 *Information Operations* (IO) (U) (9 December 1996).
(4) DoD, CJCSI 6510.01B *Defensive Information Warfare Implementation* (22 August 1997).

DoD Component	Functions	Defensive Information Operations Responsibilities
CINCs	• Maintain security of the command • Protect the United States • Maintain preparedness • Carry out assigned missions, assign tasks and direct coordination to ensure unity of effort • Communicate with the Services, SECDEF and subordinate elements • Advise CJCS of significant events • Exercise combatant command through components, subordinate unified commands, and joint task forces.	• Plan/execute IW across full range of military operations • Develop effective indications and warning methods • Integrate IW capabilities into deliberate and crisis plans • Develop process that integrates IW disciplines within the CINC/Joint Task Force staffs (IW Cell) • Implement education, training, and awareness program • Integrate IW-D procedures, processes, and capabilities into daily operations • Develop, coordinate and execute response to IW attacks • Exercise IW-D capabilities in realistic exercises?
CJCS / Joint Staff	• Principal military advisor to President • Provide strategic direction and planning • Prepare and review contingency plans • Advise on requirements, programs and budget • Develop doctrine and formulate policy on military education and training • Direct the Joint Staff • Transmit communications between NCA and combatant commands • Determine adequacy and feasibility of plans • Seek advice of Joint Chiefs of Staff.	• Include IW concepts in Joint / Service school curricula • J2 (DIA) - Provide intel support to CINCs for IW-D planning and execution • J3 - Develop joint IW doctrine, coordinate with J6 for IW-D support to operations, provide focal point for coordinating CINC response to IW attack • J6 - Coordinate with J7 to integrate IW-D capabilities into deliberate and crisis planning; develop IW-D doctrinal concepts; coordinate with Services to validate CINC requests to release COMSEC material; establish and chair IW-D panel under MCEB.
Service Chiefs	• Prepare forces and establish reserves of manpower, equipment, and supplies • Maintain mobile reserve forces • Recruit, organize, train and equip interoperable forces • Prepare and submit budgets • Provide bases and installations • Furnish administrative and logistic support for all forces and bases • Assist each other in accomplishment of their respective functions.	• Conduct RDT&E • Organize forces with IW capabilities • Integrate IW-D concepts into Service doctrine • Exercise IW-D capabilities in realistic exercises.
Director, NSA	• Provide intelligence support, technology, and advice.	• Oversee administration of National Security Information Systems Incident Program, i.e., coordinate with Defense Information Systems Agency (DISA) and DIA to integrate these efforts with those to protect the DII • Develop and promulgate technical criteria, standards, and guidelines for certification of national security systems.
Director, DIA	• Provide intelligence support.	• Provide intelligence assistance to combatant commands • Conduct analysis of IW threat information • Provide precise and timely intelligence to combatant commands, DISA, NSA, and Joint Staff • Identify intelligence requirements.
Director, DISA	• Ensure the DII contains adequate protection against attack.	• Establish a security architecture and standards for protecting DII • Develop security incident program and response capability • Ensure the DII contains adequate protection against attack • Provide technology and services to ensure availability, reliability, maintainability, integrity, and security of the DII • Assess vulnerabilities of defense information systems • Develop guidelines and courses; provide assistance for education, training, and awareness.
All DoD Components		• Ensure DAA identified for each national security system • Employ cryptosystems in high risk environments • Eliminate dependence on paper-based / non-electronic keying methods • Establish a Security Incident Response Capability • Develop and implement INFOSEC education, training, and awareness programs.

Exhibit 2-2-1. Functions and Defensive Information Operations Responsibilities of the Department of Defense and Its Major Components

2.3 OPERATIONS

As suggested in Section 2.1, the strategy, policy, and doctrine for defensive information operations are evolving. Consequently, the current state of the operational art is based on current practice and lessons learned from operational experience, exercises, and war games.

Defensive information operations are heavily dependent on intelligence support. This support includes threat assessments and dissemination, indications and warning, and current intelligence. The capabilities of the intelligence community to provide this support are presented in Section 2.3.6.

Defensive information operations currently emphasize monitoring systems and networks. These systems and networks use audit mechanisms and detection tools to detect abnormal events that might constitute reportable incidents. The Joint Information Assurance Operations Working Group is currently developing the definitions and nature of reportable incidents (discussed in more detail in Section 3). DISA, in coordination with the Services, is developing a process for reporting and correlating incident reports and for issuing tactical warning of actual information attacks for the defense-wide community. DISA also has developed a process to integrate the incident information with the Global Command and Control System, thereby providing a first cut at integrating the defensive information operations picture with the overall operations picture of the battlefield.

The following sections briefly discuss the operations environment, emerging information threat conditions, incident reporting mechanisms, recent exercises, readiness reporting, and the relationships to and support provided by the intelligence and law enforcement communities.

2.3.1 Environment

The Global Information Environment (GIE) is an expanding domain. It consists of all organizations and resources (including persons, knowledge, and systems) that acquire, store, use (process) and transport data and information. The GIE rests upon a Global Information Infrastructure (GII) of information processing capabilities and communications connections among individuals and organizations (local, regional, national, trans-national, and international) across the globe. GII communications connections are now dominated by electronic modes (physical forms), media (physical paths for movement), and methods (patterns of distributing information, including broadcast, point-to-point, and multipoint network). Different **modes** (such as analog and digital) are integrated to provide greater variety and flexibility in the transport and use of information. Innovations in **media**, such as fiber-optic cables, communications satellites, and wireless cellular transmitter-receiver structures, have introduced huge increases in communications carrying capacity and offered unprecedented mobility to end users. Different media (such as wireline, fiber-optic, and radio spacewave) are integrated into hybrid networks. The linkage of such communications infrastructures with specialized and general-purpose computer microprocessors has launched revolutionary changes in the amount, speed, cost, and variety of information's form and function. It also has dramatically changed the availability and distribution (including extension, or reach) of information use across social, economic, political, and geographical boundaries. The pace of life is faster: traditional delays

caused by slower communications and manual information processing and computation are fading. These trends will surely continue to accelerate.

The U.S. Armed Forces are enmeshed in a Military Information Environment (MIE) which is a subset of the GIE. The MIE consists of the friendly and adversary, military and nonmilitary, information systems and organizations, both that support, enable, or significantly influence a specific military operation. It reaches across space from the home station to the area of operations (AO), across time from alert through redeployment, and across purposes from tactical missions to economic or social end states. "[B]attlespace now includes global information connectivity." [18]

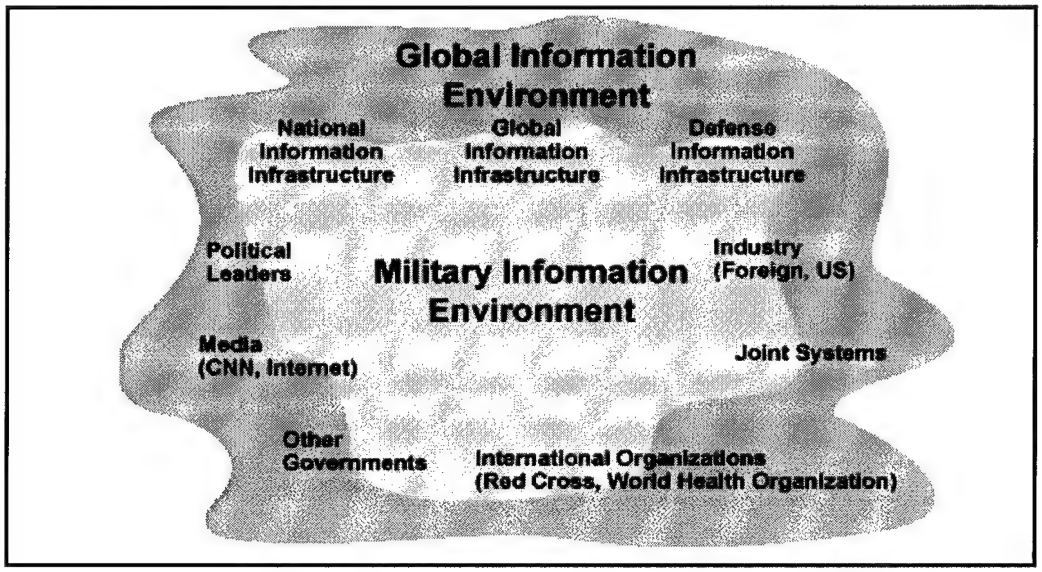


Exhibit 2-3-1. The Military Information Environment within the Global Information Environment [19]

The physical and organizational infrastructure supporting the military forces is the DII, which is a part of the larger National Information Infrastructure (NII) within the GII. The DII encompasses data processing and transfer resources, including storage, manipulation, retrieval, and display. It connects DoD mission support, command and control (C2), and intelligence computers and users through voice, data, imagery, video, and multimedia services over the Defense Information Systems Network (DISN). The DII is also embedded within and deeply integrated into the NII. The seamless relationship between DII and NII makes distinguishing between them impossible. The merging of military and civil information networks means that fixed boundaries in the information environment are not easily identifiable.

The natural environment (weather, geological activity, etc.) and manmade physical environmental supports (electrical power outages, leaking water pipes, flooding, etc.) continue

[18] Department of the Army, Field Manual 100-6 *Information Operations* (27 August 1996). Available from U.S. Army Training and Doctrine Command Training and Doctrine Literature home page Internet site at http://www.atsc-army.org/atdls.html.
[19] Ibid.

to present a threat to the information environment. But a rapidly growing threat, created through increased access to interconnected networks, is that of the human agent.

Human agents may be intra-organizational users ("insiders," disgruntled employees, etc.), terrorists, political opponents, foreign military or intelligence/covert action/special operations services, business organizations, and individual and group "hackers." The means of carrying out the attack vary, from physical attack, to radiated electromagnetic energy, to malicious software code, or sophisticated use of intrusion tools and techniques to gain access via communications entry points. Objectives and purposes range from gaining information for intelligence and industrial espionage reasons, theft, sabotage, to even malicious mischief. It would not be prudent to think that our critical information infrastructures would go unchallenged from these threats. In the future, technical and operational weaknesses (including human error), and vulnerabilities will multiply. The threats will correspondingly become "more complex, sophisticated, and perhaps more clandestine." [20]

There must be a response to those threats. We must attain Information Assurance — the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. "[I]nformation superiority will require ... defensive information warfare (IW) ... to protect our ability to conduct information operations." [21] This protection includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Defensive information operations need to be conducted through information assurance (IA), physical security, counter-deception, counter-PSYOP, counterintelligence (CI), electronic protection (EP), and special information operations (SIO). [22]

A more DoD-centric view of the environment has resulted from recent operational experience in incident reporting and warning. Exhibit 2-3-2 shows this view. The exhibit portrays the incident reporting and warning environment. While actual incident reporting and warning procedures are under development, the reader should realize the complexity of the process and the breadth of organizations that are stakeholders in the process. The view includes a notional representation of the basic national, CINC, and Service operations centers.

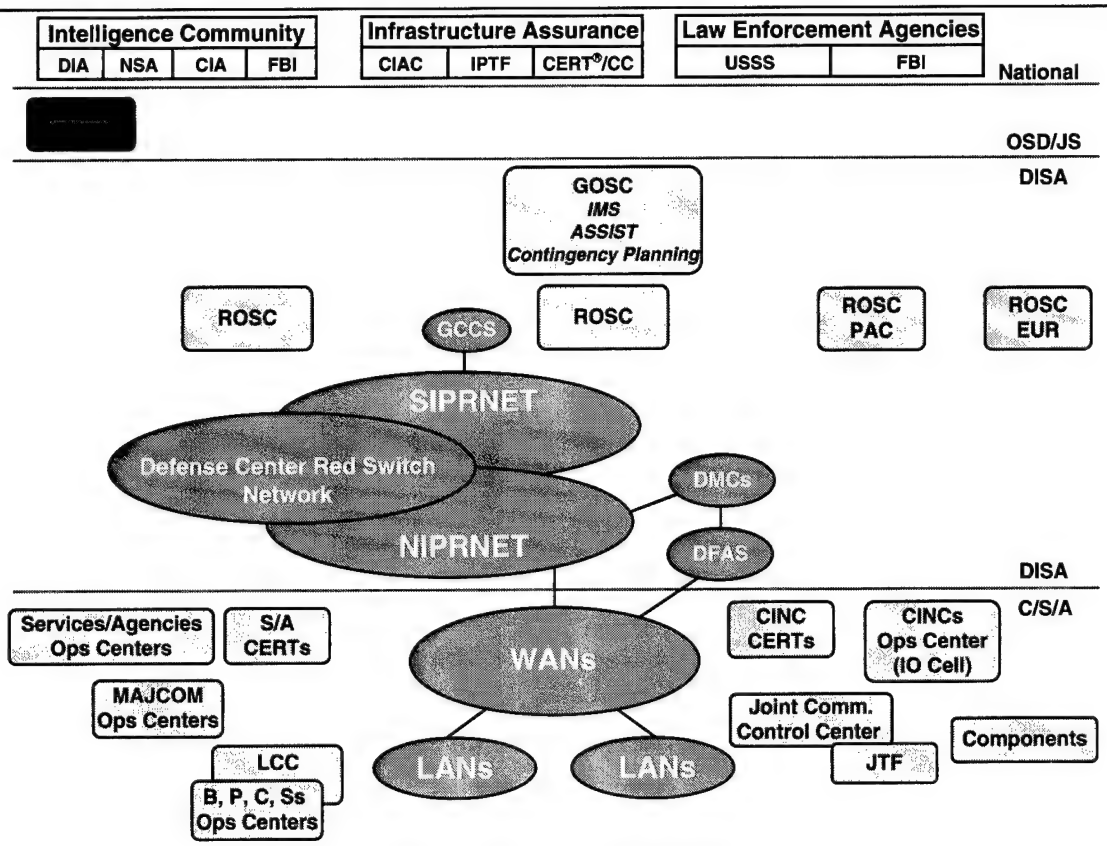
The exhibit has been divided into four horizontal sections to show the responsibilities of each of the operations centers. The basic information operating elements, which are the focus of defensive information operations, are shown as elements of the DII and local and deployed elements. The local and deployed operating elements are generally also considered to be elements of the DII, but specific responsibilities and authorities for operation and control of these elements has not yet been delineated. The exhibit shows only a few examples of these elements — the actual composition of the DII and the C4ISR support structure is obviously much more extensive, detailed, and complex than is shown here.

---

[20] DoD, The Joint Staff, *Concept for Future Joint Operations* (undated). Available from Joint Staff site on Internet at http://www.dtic.dia.mil/doctrine/jv2010/concept.html

[21] *Joint Vision 2010* (undated), p. 16.

[22] Joint Publication 3-13 *Joint Doctrine for Information Operations*, Second Draft (2 July 1997).



LEGEND:

ASSIST	- Automated System Security Incident Support Team	IPTF	- Infrastructure Protection Task Force
B,P,C,Ss	- Bases, Posts, Camps, Stations	JTF	- Joint Task Force
C/S/A	- CINCs/Services/Agencies	LCC	- Local Control Centers
CERT®/CC	- Computer Emergency Response Team/ Coordinating Center	MAJCOM	- Major Commands
		NIPRNET	- Unclassified but Sensitive Internet Protocol Routing Network
CIAC	- Computer Incident Advisory Capability		
DFAS	- Defense Finance & Accounting Service	NMCC	- National Military Command Center
DMCs	- Defense Megacenters	PAC	- Pacific
EUR	- Europe	ROSC	- Regional Operations & Security Centers
GCCS	- Global Command and Control System	S/A	- Services/Agencies
GOSC	- Global Operations and Security Center	SIPRNET	- Secret Internet Protocol Routing Network
IMS	- Integrated Management System	USSS	- U.S. Secret Service

Exhibit 2-3-2. The Current DoD Defensive Information Operations Environment

A Local Control Center at the bases, posts, camps, and stations operated by the Services controls the local operating elements. The Joint Communications Control Center, operated by the Joint Task Force, controls the deployed operating elements. DISA, in its role as the central manager of the DII, controls regional and global operating elements through the Global Operations and Security Center (GOSC).

Support to defensive information operations is provided by the intelligence community, the law enforcement community, and an emerging infrastructure protection community discussed briefly in Section 3.2.1. For simplicity, only the national-level elements of these communities are depicted. Many organizations throughout the organizational structure of DoD and at the national, state, and local levels support these communities.

The LCCs, ROSCs, and GOSC exercise operations control of the information operating elements on the basis of network and systems management and security information reported to the centers. This network and systems management information includes information such as faults, performance trends, and configuration of system and network elements. Historically, security control of the operating elements has been exercised at the lowest operating level. With the increase in inter-networking, a security management infrastructure that would exercise security control on a regional or even a global basis is needed.

Information operations incident within the local, deployed, and DII operating elements are reported in parallel to the DII control centers and to the local or regional computer incident response teams (referred to as IRTs) that have been established by the CINCs and the Services. In some cases, these response teams have established liaison with or have on-site representatives from the supporting intelligence and law enforcement organizations. These liaisons aid in sharing the incident information and in prosecution of the perpetrator of the incident. The incident reports are then passed up to the Service IRT, the ROSCs, and the GOSC for correlation with other incident reports and sharing with appropriate intelligence, law enforcement, or infrastructure assurance organizations. These reports are analyzed for possible impact on all the operating elements and, as appropriate, warnings are disseminated down through the reporting channels. As appropriate, these incident reports are integrated into the operations picture.

The complexity of the environment demands a rational approach to operations. The Joint Staff policy on defensive information warfare implementation [23] suggests that the process for information protection involves determining: what should be protected based on the value of the information collected, processed, displayed, etc.; how the necessary protection should be afforded; and to what extent the protection should be applied. The "what" is referred to as "scope;" the "how" and "to what extent" are referred to as "standards." Such a risk management approach requires specific procedures. At the joint level, neither the policy nor other documented guidance provides the specific methods and tools needed by the operating forces to determine the scope and standards of information protection. This is particularly true for unclassified and unclassified but sensitive information. In recognition of this, the Information Assurance Division of the Joint Staff began to explore the possibility of developing a process for determining scope and standards. As a first step, a research report on the state of information risk management models, methods, and efforts was recently completed. [24]

---

[23] DoD, CJCSI 6510.01B *Defensive Information Warfare Implementation* (22 August 1997).

[24] DoD, The Joint Staff, Information Assurance Division (J6K), *The State of Information Risk Management Methodology*, by Science Applications International Corporation (SAIC) (8 August 1997).

The DoD Director of Net Assessment also is attempting to define more thoroughly the nature of the information operations environment. A preliminary net assessment focuses on a single potential opponent in an effort to test the approach, and looks out to the year 2010 or so. The assessment is based on military function, i.e., it does not ignore other trends affecting the information environment or other aspects of the national security, but it focuses on military operational issues. The assessment, as a preliminary effort, will help set the agenda for any follow-on effort. The agenda will probably include both looking at additional opponents, and assessing in more detail some of the trends data (*inter alia*). Additional efforts will depend on the resulting conclusions.

2.3.2 Information Alert Conditions

As suggested earlier, one of the challenges in implementing the defensive information operations model has been the lack of an adequate alerting mechanism. As in the traditional operations community, the defensive information operations community requires an alerting mechanism to heighten awareness and preparedness as the threat increases. In addition, the community should probably respond in a prescribed manner to increasing threat conditions. Such responses might include minimizing the traffic on the networks, restricting personnel access to operational facilities, disconnecting certain systems from networks that are likely targets, and possibly implementing wartime modes of operation. Exhibit 2-3-3 provides an example of these information threat conditions and responses. These examples are based on the Report of the Defense Science Board Task Force on Information Warfare - Defense [25] and a draft prepared by USSTRATCOM. [26] As suggested by USSTRATCOM, "The decision to change the information threat condition is based on several factors which include the assessed threat, the capability to implement the required protective measures, as well as the overall impact the action will have ....". [27] The Joint Staff J2 also is attempting to define these conditions formally for the defensive information operations community.

---

[25] DoD, Office of the Under Secretary of Defense for Acquisition and Technology, Defense Science Board (DSB), *Report of the Defense Science Board Task Force on Information Warfare - Defense* (November 1996).
[26] United States Strategic Command, *Information Operations Threat Conditions Definitions and Measures Proposal* (15 May 1997).
[27] Ibid.

Condition	Situation	Response
Normal	• Normal threat - criminal/ incompetents • Normal activities in all sectors • Routine security posture	
ALPHA Simple Activity	• General threat of possible information attack • Slight increase in incident reports • Slight increase in regional or functional events • Probes indicating random surveillance/reconnaissance	• Remind personnel of security responsibilities • Increase review of firewall and operating system audit logs • Close remote maintenance ports on routers, firewalls, servers, telephone switches • Begin specialized incident and readiness reporting • Consider need for crisis action team
BRAVO Significant Activity	• Increased, more predicable threat of information attack • Significant increase in incident reports • Increase of nuisance viruses, social engineering, network pinging • Slight increase in regional or functional events	• All above responses implemented • Augment emergency response centers with security analysis capabilities • Turn on real-time audit capability • Place ISSMs and ISSOs on alert status • Disconnect all unnecessary access (e.g., commercial Internet/WWW) • Consider disconnecting secure mail guard • Official business conducted via classified media only • Restrict use of radios and cellular phones • Form crisis action team • Consider need for battle staff
CHARLIE Serious Activity	• Actual information attack occurs - denial of service, attempted/actual access, system/network control, data manipulation, etc. • Major regional or functional events which undermine U.S. interests • Events correlated to foreign powers	• All above responses implemented • Form battle staff • Disconnect secure mail guard • Limit use of non-secure and secure media • Begin aggressive forensics • Consider declaring state of emergency
DELTA Brink of War	• DEFCON or Terrorist THREATCON warrant extreme measures • Increased severity of information attack • Efforts required to maintain or restore minimum services to accomplish war-fighting mission • Events attributable to hostile foreign governments	• All above responses implemented • Declare state of emergency • Disconnect critical elements capable of standalone operation • Implement special protocols

Exhibit 2-3-3. Example Information Alert Conditions and Responses

2.3.3 Incident Reporting

The Joint Information Assurance Working Group is developing definitions of defensive information operations events and incidents and recommended reporting actions for various categories of incidents. Exhibit 2-3-4 shows examples of the incidents and possible reporting actions. The actual reporting action for each incident varies with the seriousness of the incident. For the purpose of incident reporting, an event is defined as "Any suspicious pre-assessed activity" while an incident is defined as "An assessed event of attempted entry, unauthorized entry, and/or an information attack on a Automated Information System (AIS). It includes unauthorized probing, browsing, disruption, or denial of service; altered or destroyed input, processing, storage, or output information; or changes to system hardware, firmware, or software characteristics with or without the user's knowledge, instruction or intent (e.g., malicious logic)." [28] For example, all reporting actions would take place for an unauthorized privilege (root) while a malicious logic incident causing the isolation of a single machine would be reported only to the systems administrator and the appropriate DoD IRT.

Event/Incident	Possible Reporting Actions
• Unauthorized Privileged Access (Root) • Unauthorized User Access • Unauthorized Unsuccessful Attempted Access – Simple – Significant – Serious • Unauthorized Probe/Reconnaissance – Simple – Significant – Serious • Poor Security Practices – Classified System – Direct Root Login – All Others • Denial of Service Information Attack • Malicious Logic – Isolation of Base, Post, Camp, Station – Isolation of Organization from Network – Isolation of Single Machine • Policy Violation • Other Suspicious Activities	• Open an Incident Report • Contact Systems Administrator • Contact Security Officer • Report to Local Control Center • Report to Local Commander • Contact Appropriate DoD IRT • Report to Regional Operation and Security Officer • Report to Major Command Operation Center • Conduct DISA/ASSIST-CITAC-NSA/IPO Event Conference • If Commercial, Contact CERT®/CC • Add Intruder IP Source to Hot List • Post Attack Profile to GCCS/SIPRNET • Contact NMCC/CINCs • Report to Law Enforcement Agencies

Exhibit 2-3-4. Example Incidents and Possible Reporting Actions

Exhibit 2-3-5 shows the defensive information operations reporting and warning environment, along with a simplified version of the reporting channels. The actual reporting channels are still being developed.

---

[28] DoD, DISA, *Joint Information Assurance Operations Working Group (JIWG),* Briefing by Major Dexter R. Handy (31 July 1997).

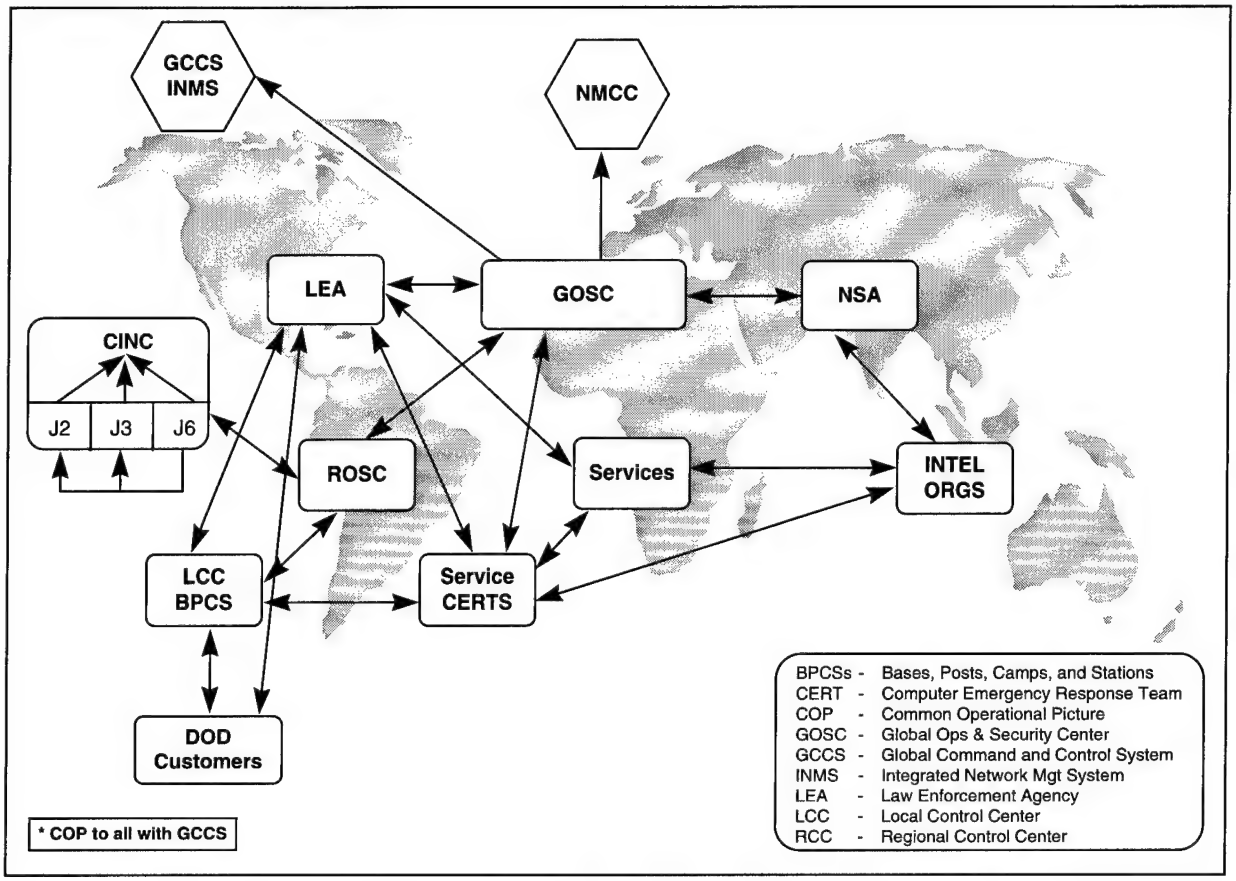


Exhibit 2-3-5. Defensive Information Operations Reporting and Warning Environment

2.3.4 Exercises and War Games

Exercises and war games related to information assurance are being used to better define the environment, the threat conditions, and the reporting processes. These exercises and war games have been conducted by the President's Commission on Critical Infrastructure Protection, the Office of the Assistant Secretary of Defense (C3I), the Joint Staff, and the United States Atlantic Command, among others. While most of the details of these exercises and war games are classified, the following unclassified discussions provide some insights into the environment and challenges involved.

The President's Commission conducted what are referred to as "prosperity games" for the purpose of identifying infrastructure protection issues which cut across the critical infrastructures. [29] The games were conducted in cooperation with the National Communications System, the Department of Energy, and the Sandia National Laboratories Surety Program Office. Some of the issues identified include the need for:

[29] Department of Energy, Sandia National Laboratories, *U.S. Infrastructure Assurance Prosperity Game™ Summary*, Briefing to NSTAC IES (22 May 1997).

- Data collection, analysis, and threat sharing
- Response capability
- New risk management tools, models, and techniques
- Security standards
- Education and awareness.

United States Atlantic Command has engaged in a series of exercises titled Evident Surprise. These exercises have focused on the entire spectrum of information operations, with emphasis on the special aspects of information operations such as intelligence support, policy interagency coordination, and legal authorities. The exercises have resulted in refinement of some of the evolving strategies and definition of the operating environment.

According to a recent article, "unauthorized users can gain 'super user' access to vital, and ostensibly secure, systems, according to Pentagon sources." [30] The article went on to state that "another Joint Staff source explained the military purposefully let down its guard to see what would happen if indeed such a terrorist action took place." [31]

Because of the complexity of information operations and the incomplete doctrine and tactics for conducting information operations, exercises and war games will continue to play a key role in the development of policy, doctrine, and tactics.

2.3.5 Readiness Reporting

Defensive Information Operations should be viewed from a warfighting perspective. Operational forces should be able to detect, differentiate among, warn of, respond to, and recover from disruptions of supporting information services. Recovery from disruptions resulting from failures or attacks might involve repair, reconstitution, or the employment of reserve assets. In some cases, network managers may have to isolate portions of the network, including users of the network, to preclude the spread of disruption. Given the speed with which disruptions can propagate through networks, these capabilities may need to be available in automated form within the network itself. Finally, there must be some means to manage and control these capabilities. These are all a part of operational readiness.

An essential element of operational readiness is a standardized process to enable commanders to assess and report their operational readiness status as it relates to their specific dependency on information and information services. A standard vocabulary will enable common description of risk scenarios and assessment methodologies. The use of a structured assessment and reporting process will help identify discrete information and information service dependencies. This process will move information assurance from a global and unsolvable problem quantifiable risks to specific information-dependent activities within a commander's sphere of

---

[30] "Joint DoD Exercise Reveals Military IW Vulnerabilities," *Defense Information and Electronic Report* 2 (11 July 1997) 28:1.
[31] Ibid.

responsibility. Supporting elements and the commercial sector can apply a similar assessment and reporting process as well.

For example, defensive information operations factors could be added to the following Joint Reporting System elements and joint doctrine: [32]

- SORTS (Status of Resources and Training System), Joint Pub 1-03.3 - Add DIO preparedness to overall unit readiness rating (C-Level).
- CSPAR (CINCs Preparedness Assessment Report), Joint Pub 1-03.31 - Add explicit review of DIO to review of operations and contingency plans.
- CSAAS (Combat Support Agency Assessment System), Joint Pub 1-03.32.1 - Address DIO preparedness in new **annual** CSAAS cycle.
- Joint Tactics, Techniques and Procedures for Base Defense, Joint Pub 3-10.1 - Include DIO, apply to CONUS and OCONUS bases.
- Joint Doctrine for Operations Security, Joint Pub 3-54 - Add DIO posture to assessment factors.
- DISA Communications Spot & Status Reports, Joint Pub 1-03.10 - Modify to include status reporting on major computing resources, include CINCs, Services and Defense Agencies, Military Departments mobilization and sustainment assets.

2.3.6 Intelligence Support

Previous editions of this report have noted the importance of intelligence support to information assurance. This and other reports and study groups have identified the need for the Intelligence Community (IC) to adopt new organizations, procedures and techniques to provide this support. This section provides a thumbnail sketch of the IC organization, roles, and responsibilities to help the reader understand the challenges of IC support to information assurance.

Scientific and technical intelligence [33] and counter-intelligence [34] are of special value in information assurance because they give special attention to threat capabilities against friendly information systems. Capabilities of potential adversary forces and systems cannot be described or evaluated without intelligence assessment of and reference to vulnerabilities of friendly organizations, resources, and actions.

---

[32] Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare - Defense.*

[33] Focuses on foreign research and engineering techniques and characteristics, capabilities, and limitations of systems, materiel, and production methods. Joint Publication 1-02 *DoD Dictionary.*

[34] Conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Joint Publication 1-02 *DoD Dictionary.*

The IC refers in the aggregate to those Executive Branch organizations that conduct the U.S. national intelligence effort. The head of the IC is the Director of Central Intelligence (DCI). Exhibit 2-3-6 lists organizations that support the DCI and the Community. Exhibit 2-3-7 shows the membership of the IC. [35]

- Intelligence Community Executive Committee(IC/EXCOM)
- Community Management Staff (CMS)
- National Intelligence Council (NIC)
- DCI's Counterterrorist Center
- National Counterintelligence Center (NACIC)

Exhibit 2-3-6. Organizations Supporting the DCI and the IC [36]

Service-specialized IW elements also perform significant intelligence roles:

- U.S. Army Land Information Warfare Activity (LIWA) [37]
- Naval Information Warfare Activity (NIWA)
- Fleet Information Warfare Center (FIWC)
- Air Force Information Warfare Center (AFIWC). [38]

Although not formally identified as part of the IC, other organizations also perform important intelligence functions. For example, the commanders in chief (CINCs) of combatant commands (unified and specified) operate Joint Intelligence Centers (JICs) to perform intelligence planning, control, and analysis functions. Intelligence components of subordinate joint forces and Service components of joint forces support the JIC.

The following is a general overview of intelligence activities and organizations. It would be beyond the scope of this report to describe in further detail the complex real-world architectures of operational environments and interrelated organizations, resources, and activities of the various parts of the IC, even those one might identify as related only to IA support. Certain aspects, such as computer incident reporting, have already been touched upon. The main functions of intelligence are cyclic, iterative, and done in parallel: planning and directing the effort, collecting data and information, processing and analyzing data and information to produce intelligence, then disseminating then to users or consumers.

---

[35] Consult "United States Intelligence Community," on United States Office of the Director of Central Intelligence Internet site at http://www.odci.gov/cia/other_links/wheel/index.html for descriptions of each major component

[36] See NACIC Internet site at http://www.nacic.gov/ Also, the DCI has established a number of centers, the Counterterrorist Center and Counterintelligence Center being two.

[37] U.S. Department of the Army, Field Manual 100-6 *Information Operations* (27 August 1996). Available on Internet at http://www.atsc-army.org/atdls.html

[38] U.S. Department of the Air Force, USAF Fact Sheet 95-10 "Air Intelligence Agency" on USAF website at http://www.af.mil/news/factsheets/Air_Intelligence_Agency.html . Also, see U.S. Department of the Air Force, Air Information Warfare Center (AFIWC) Internet site at http://www.aia.af.mil/aialink/homepages/afiwc/index.htm

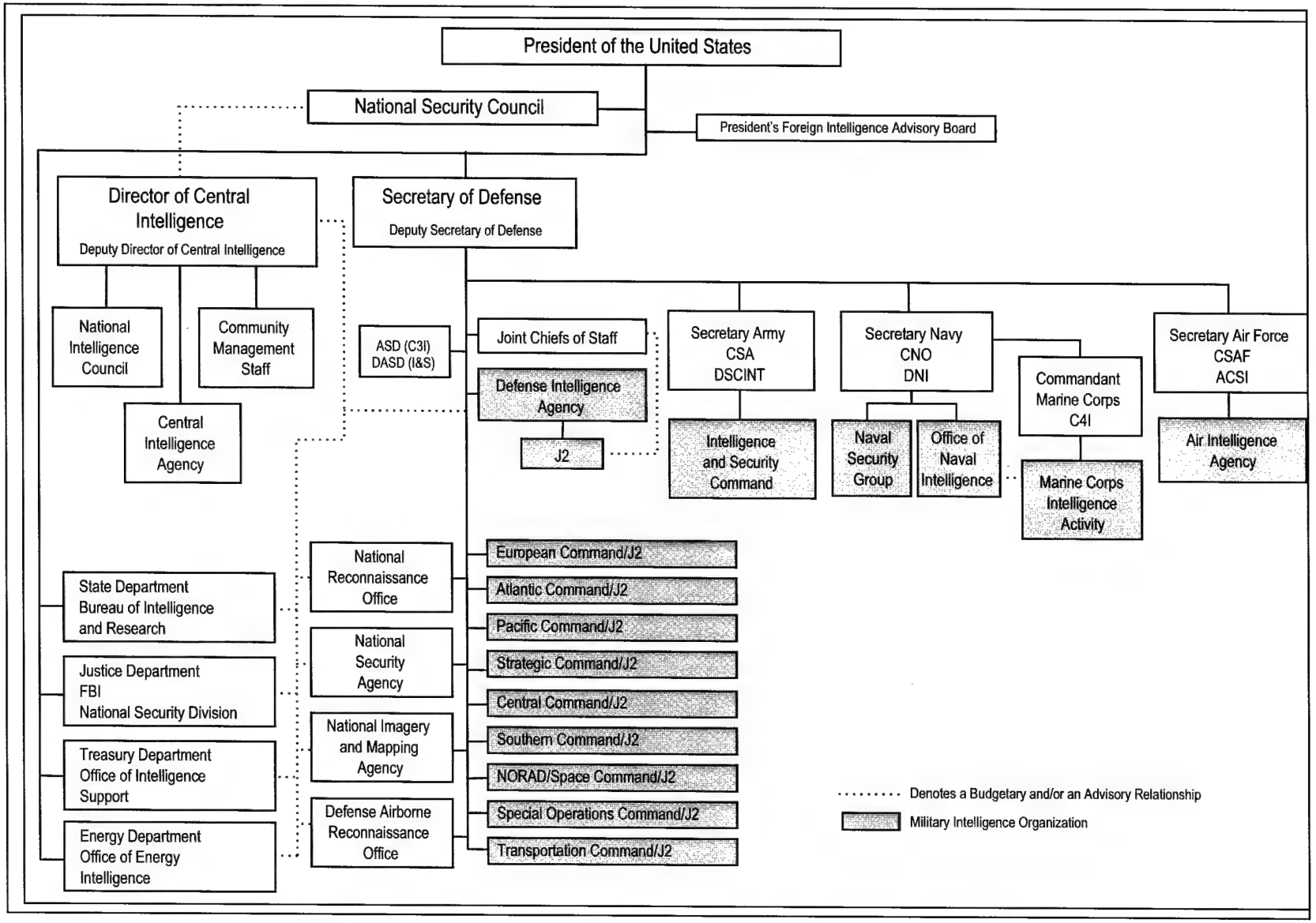


Exhibit 2-3-7. Organization Chart View of the Intelligence Community [39]

[39] U.S. Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1 March 1996).

Intelligence, like security, is for everybody. Interagency cooperation is increasingly important. Support to IA generates requirements and actions that have to compete with other priority and routine tasks. These tasks are performed not only internally within and among IC component staff and line organizations, but also externally in concert with other staffs and line organizations. Collectors and producers are also consumers. Intelligence is a distributed function performed not only by specialized elements, but also by a wide variety of organizations. Any unit report of a computer network attack provides information, which in turn feeds into a specialized intelligence process and ultimately contributes to the larger intelligence function. Operational activities and communications/information exchange arrangements and activities are extensive and complicated. Joint Publication 2-0 *Joint Doctrine for Intelligence Support to Operations* [40] provides a comprehensive description of joint architectures.

Cumulatively, intelligence provides basic encyclopedic intelligence for planning, threat information to support training as well as system and force development, and current intelligence for indications and warning and the conduct of more immediate operations. Any organization performing IA functions must draw from available relevant intelligence. If more is needed, then a Request for Information (RFI) should be submitted. The discussion of doctrine, below, spotlights what elements of intelligence are important in what ways to the elements of IA.

A series of statutes and Executive Orders provides legal authority for the conduct of intelligence activities. The *National Security Act of 1947* as amended (50 U.S.C. 401 et seq.) provides the basic organization of the U.S. national security effort. Executive Order 12333 [41] has guidelines for the composition of the IC and the conduct of intelligence activities. CIA is to collect, produce, and disseminate foreign intelligence and counter-intelligence, including information not otherwise obtainable. The Departments of Defense, Treasury, State, and Energy are given certain authorizations to collect foreign intelligence. NSA is authorized to collect signals intelligence for foreign intelligence purposes. FBI may collect foreign intelligence within the United States, when requested by officials following stated procedures.

The FBI has the main responsibility for counter-intelligence in the United States. Generally, other departments or agencies must coordinate counter-intelligence activities outside the United States with the CIA, and within the United States with the FBI. The United States Secret Service in the Department of Treasury is allowed electronic surveillance activities to protect the President and selected others. The *Foreign Intelligence Surveillance Act of 1978* provided important rules on electronic surveillance on agents of foreign powers. Executive Order 12139 (23 May 1979) *Exercise Of Certain Authority Respecting Electronic Surveillance* [42] directed implementation of the *Act*.

---

[40] DoD, The Joint Staff, Joint Publication 2-0 *Joint Doctrine for Intelligence Support to Operations* (5 May 1995).
[41] The President, Executive Order 12333 *United States Intelligence Activities* (4 December 1981), available on Federation of American Scientists Internet site at http://www.fas.org/irp/offdocs/eo12333.htm
[42] The President, Executive Order 12139 (23 May 1979) *Exercise Of Certain Authority Respecting Electronic Surveillance,* available on Federation of American Scientists Internet site at http://www.fas.org/irp/offdocs/eo12139.htm

Concerning "special activities" and covert operations, Sections 503 and 504 of the *National Security Act of 1947* and 50 U.S. Code 413b and 414 require that no department or agency may expend funds on a covert action unless the President has signed a written "finding" that the covert action is necessary and important to national security. Furthermore, no agency except CIA (or the Armed Forces in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective.

Joint Vision 2010 outlined emerging operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. These concepts require a foundation of improved command, control, and intelligence ensured by information superiority. Defensive information operations will be one of our biggest challenges in providing that information superiority.[43] The *Concept for Future Joint Operations* ,[44] a refinement and extension of *Joint Vision 2010*, observes that the focus of IO is on vulnerabilities and opportunities presented by increasing dependence on information and information systems. We must remain vigilant to rapid changes in information and information systems and how we or our potential adversaries might apply such changes to future conflict. Full-dimension protection requires awareness of potential adversary technologies and capabilities and of vulnerabilities on both sides; anticipation of enemy actions; and rapid dissemination of threat information to all forces. Adding to the set of emerging concepts in the Information Operations domain is a Joint Staff brochure, *Information Warfare: A Strategy for Peace... The Decisive Edge in War.*[45] This brochure emphasizes that Defensive IW (IW-D) requires a process to identify threats, attacks, or other degrading conditions and to disseminate warnings. Risk assessment processes consider system vulnerabilities and threats posed by both potential adversaries and by natural phenomena. Threat knowledge includes identities and intentions of attackers, attack techniques and methods, and potential targets. Defending against an attack is predicated on how well the intelligence threat and associated indications and warning processes function.

Intelligence support is also featured in emerging doctrinal concepts. New doctrine on Information Operations to implement the concepts reflected in *Joint Vision 2010*, the *Concept for Future Joint Operations,* and *Information Warfare: A Strategy for Peace... The Decisive Edge in War* is in preparation. When published, Joint Publication 3-13 *Joint Doctrine for Information Operations*[46] will provide important new guidance to IO and the role of intelligence in IO. This publication observes that early identification of specific targets is essential to defensive IO. Furthermore, defensive IO risk management must consider vulnerabilities and threats. Intelligence understanding of the threat should be in terms of specific adversary intent, capability, and opportunity to influence adversely those elements of the friendly information environment that are critical to achieving objectives. Readily accessible, timely, accurate, and sufficiently detailed intelligence support is critical to planning, execution, and assessment of IO. Intelligence contributes to defensive IO counterdeception, counter-psychological operations, and actions against espionage, sabotage, and terrorism.

---

[43] DoD, *Joint Vision 2010.*
[44] DoD, *Concept for Future Joint Operations.*
[45] DoD, The Joint Staff, *Information Warfare: A Strategy for Peace... The Decisive Edge in War* (1996).
[46] DoD, Joint Publication 3-13 *Joint Doctrine for Information Operations,* Second Draft (July 1997).

To reflect and apply Joint Vision 2010 to the Army, *Army Vision 2010* [47] emphasizes that information operations (IO) conducted to gain information dominance are essential to **all** operations. Field Manual 100-6, *Information Operations*, [48] contains important new doctrine on Information Operations and intelligence. This document introduces the concept of *relevant information*: information from the military information environment that significantly affects, contributes to, or is related to the execution of the operational mission at hand. *Intelligence* is the critical subelement of relevant information that focuses primarily upon foreign environments and the adversary. The first critical step in protecting IO capabilities is to identify specific and potential threats. Commanders ask how the adversary can employ destruction, EW, military deception, OPSEC, and PSYOP to disrupt our C2 systems and decisionmaking processes. A risk management process is based on identification of such factors as specific threat capabilities, technical capabilities, doctrine, and past performance of the threat force. Threat and vulnerability assessments are essential to risk management and are integrated into a detailed procedure. The Army's draft Field Manual 34-40, *Intelligence-Electronic Warfare Support to Command and Control Warfare,* [49] currently in progress, is expected to address intelligence support to this central component of Information Operations.

The Navy Naval Doctrine Publication 2, *Naval Intelligence*, [50] states that the commander must execute offensive and defensive force protection, supported by all intelligence functions. Naval intelligence identifies adversary intelligence capabilities; assesses friendly vulnerabilities; identifies risk; and enables planning for operational security, deception, and surprise. Indications and Warning (I&W) are needed against hostile attack. Successful IW/C2W must be based on sound, fused, all-source, rapid intelligence.

The Air Force recent publication, *Global Engagement: A Vision for the 21st Century*, [51] observes that dominant battlefield awareness will depend heavily on the ability of Air Force assets to provide global awareness and intelligence support. The top IW priority is to defend our own increasingly information-intensive capabilities. Air Force Doctrine Document 50, *Intelligence*, [52] affirms that intelligence is a primary contributor to information dominance and that a commander's first objective is to control the environment. To enable this control, intelligence provides required detail on foreign air, space, and IW capabilities.

Several classified and unclassified intelligence and threat products have been published in the last year. Most importantly, the National Intelligence Council (NIC) published a new National Intelligence Estimate (NIE) on foreign Information Warfare activities on 21 July 1997, classified Secret/No Foreign Dissemination. A Sensitive Compartmented Information (SCI) version will be published in August 1997. The NIC is considering an unclassified version. [53] Also, the

---

[47] Department of the Army, *Army Vision 2010* (undated) available on Internet at http://www.army.mil/2010/

[48] Department of the Army, Field Manual 100-6 *Information Operations.*

[49] Per phone conversation with W. Horlick of USAIC on 1 July 1997.

[50] Department of the Navy, Naval Doctrine Publication 2 *Naval Intelligence* (undated), available on Federation of American Scientists Internet site at http://vwww.clark.net/fas/irp/doddir/navy/ndp2.htm

[51] Department of the Air Force, *Global Engagement: A Vision for the 21st Century Air Force*, on Internet site maintained by Headquarters, U.S. Air Force at http://www.xp.hq.af.mil/xpx/21/nuvis.htm

[52] Department of the Air Force, Air Force Doctrine Document 50 *Intelligence* (1 May 1996). Available on Federation of American Scientists Internet site at http://vwww.clark.net/fas/irp/doddir/usaf/50.htm

[53] Interview, NIC officer, 18 July 1997.

President, based on materials developed by the IC, submitted the first *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* in July1995, which was updated in 1996. [54] In addition, the IC will soon publish a major study on I&W for IO. [55]

In the 2nd edition of this report, a center combining various IW disciplines was being considered and described as an emerging organization. The Information Operations Technology Center (IOTC) has been established and is in early stages of organization, with an initial operating capability (IOC) anticipated in the last half of 1997. The IOTC is being formed by the joint effort of DoD and the DCI and is hosted in NSA facilities at Fort Meade, Maryland.[56] The Director, NSA, will act as executive agent.

The Quadrennial Defense Review proposed an intelligence task force, to be created by the DCI with DoD support. This task force would work with the Unified Command CINCs on a trial basis to formulate IO requirements, [57] incorporate IO into their deliberate planning process, and identify appropriate intelligence support requirements. [58] Section 3.2.1 discusses the QDR in more detail.

The National Imagery and Mapping Agency (NIMA) is an important member of the IC. It is new on the scene since the previous edition of this report. NIMA was established 1 October 1996 as a Combat Support Agency of DoD to provide timely, relevant, accurate imagery, imagery intelligence, and geospatial information. [59] These capabilities can be critical in providing I&W adversary capabilities to mount attacks against U.S. information systems. It combines the previous and disestablished Defense Mapping Agency (DMA), Central Imagery Office (CIO), and Defense Dissemination Program Office (DDPO) in their entirety; and the mission and functions of CIA's National Photographic Interpretation Center (NPIC). Also included in NIMA are imagery exploitation, dissemination and processing elements of the DIA, NRO, and DARO. [60]

In the common area between intelligence and law enforcement, the FBI established the Computer Investigation and Infrastructure Threat Assessment Center (CITAC) in 1996. CITAC's mission is to prevent, detect, and investigate computer intrusions and threats to critical infrastructures. This mission is in accordance with the critical infrastructure protection mission in Executive Order 12656 *Assignment of Emergency Preparedness Responsibilities* (18 November 1988) and Presidential Decision Directive 39 *U.S. Policy on Counterterrorism* (1995). CITAC identifies indications of foreign offensive programs, capabilities, intentions or activities targeted at critical

---

[54] Executive Office of the President, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Available on National Counterintelligence Center (NACIC) Internet site at http://www.nacic.gov/fy96rpt.htm

[55] Department of Defense, OASD(C3I) official, facsimile (10 July 1997).

[56] Interview with former Acting Director of IOTC, 30 June 1997.

[57] Interview, OASD(C3I) official, 30 June 1997.

[58] OASD(C3I) official, facsimile (10 July 1997).

[59] DoD, *DoD Organization and Functions Guidebook* (September 1996). Available on DoD Internet site at http://www.defenselink.mil/pubs/ofg.html

[60] United States National Imagery and Mapping Agency, *FACT SHEET*, from NIMA Internet site at http://www.nima.mil

infrastructures; analyzes cyber and physical threats to national critical infrastructures; and provides warning of threats.[61]

The Office of the Secretary of Defense and the Joint Staff, acting in concert, conducted the first Quarterly Technical Review on intelligence support to IO. The review permitted IO intelligence consumers and producers to identify several specific areas where intelligence support to IO may be improved. The Quadrennial Defense Review included related recommendations. [62] A DoD General Counsel opinion has been issued that penetration testing and monitoring falls within the realm of communications security (COMSEC) monitoring. In addition, the Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats met June 30-July 1. Scheduled tasks included identification of the variety of threats that should be addressed by DoD. [63]

While many of these developments are promising, a variety of issues and problems with respect to the intelligence function and its support to Information Operations and Information Assurance are still of concern to the Intelligence Community. The challenge is to prioritize tasks and optimize finite intelligence resources within an environment of competing needs and other constraints. Within the context of this broad concern, responses to a survey of IC staff and line organization officials reveal several specific issues and problems:

- Information on other country IO capabilities is not readily available.
- There is no single repository for infrastructure information.
- There has been no specific tasking to the IC for IO intelligence — a whole new type of intelligence.
- What information can be shared?
- The Intelligence Community is not well tuned to the technical import of the facts they gather. They need more technical and industry skills. They are still focused on physical observables.
- A major challenge is the ability to characterize targets, users, and implementation of information systems. The rate of innovation and change in information systems makes it difficult to characterize the specific nature of systems and their use by others (adversaries, etc.).
- CINCs look at IO intelligence needs alongside other requirements. They are accustomed to a "traditional feed." Currently, IO intelligence has no priority. Now the CINCs must consider what intelligence to "give up" in order to gain more IO intelligence.
- Intelligence is having difficulty standing up to the human factors associated with IO.

---

[61] U.S. Department of Justice, FBI, Fact sheet "CITAC Mission," provided by FBI on 10 July 1997.
[62] OASDC3I official, facsimile (10 July 1997)
[63] U.S. Government Printing Office, *Federal Register* 62 (June 23, 1997) 120. From the Federal Register Online via GPO Access at http://www.access.gpo.gov/su_docs/aces/aces140.html

- How can information collected at the "front end" be linked, correlated, fused, and leveraged into intelligence on "national level strategic attack" against infrastructures?
- IO intelligence requires a "more robust, mature, sophisticated" I&W capability beyond a simple detect and report process.
- Information protection/defense are conventionally an Information Security (INFOSEC) concern, and historically have been "outside the domain of intelligence."

2.3.7 Law Enforcement Support

Many issues related to law enforcement support must be addressed to ensure an effective and efficient information assurance capability. Law enforcement support is critical to information assurance operations for two reasons: law enforcement officials can aid in determining whether an incident is an illegal act, and, if it is, can aid in collecting the evidence necessary for a successful prosecution — a critical element of deterrence. This section focuses on coordination and information sharing in planning and responding to threats against the DII and NII.

The primary organizations providing law enforcement support to information assurance include the FBI and, to a lesser extent, the United States Secret Service at the national level. That is to say, these organizations generally have jurisdiction in interstate matters and those specifically provided for in legislation. Each of the Military Departments has criminal investigation organizations to aid in investigating computer crimes. These organizations include the Criminal Investigation Division (Army), the Naval Criminal Investigative Service (Navy), and the Office of Special Investigations (Air Force). In certain circumstances, state and/or local law enforcement officials may have jurisdiction and/or interest in information assurance incidents. Finally, at the other end of the spectrum, certain international organizations (such as Interpol) may assist in investigating information assurance incidents.

The Defense Information Systems Agency's Automated Systems Security Incident Support Team is becoming the central repository for data concerning attacks on DoD information systems. ASSIST keeps statistics on incidents and catalogs lessons learned. ASSIST reports every incident to the FBI Computer Investigations and Infrastructure Threat Assessment Center.

ASSIST is the incident response and coordination center chartered to handle all DoD INFOSEC incidents involving DoD information and telecommunications systems. As an element of DISA's Global Operations and Security Center, ASSIST provides INFOSEC incident support technical services to the entire DoD community. [64]

DISA ASSIST rarely coordinates directly with civilian law enforcement; the CITAC serves as the information coordinating body across the Government on critical infrastructure protection. Cross-agency exchange through working groups is increasing. One example of this is the Joint Information Assurance Operations Working Group, which includes many civilian agency and DoD representatives.

---

[64] As indicated in the ASSIST web page at http://www.assist.mil on 6 August 1997.

The FBI is the sole agency in the United States that determines whether an attack on a system is a terrorist attack. DISA ASSIST reports information to the FBI CITAC, which determines whether a terrorist attack has occurred. The CITAC then coordinates across the Government, reporting activities reaching specific thresholds to the Joint Staff daily.

Each of the Military Departments has formed its own computer emergency response teams. These teams are composed of highly technical personnel who are charged with helping system administrators. The teams include law enforcement representatives, some in a liaison capacity, to aid in investigating information assurance incidents.

DISA, in coordination with NSA and the Joint Staff, has been charged with developing policies and procedures to ensure all incidents are reported through appropriate channels. [65] DISA's current policy is that the system administrator who detects an incident is to notify the commanding officer, as well as the computer emergency response team. The emergency response team will immediately attempt to contain the situation. The data owner often must decide whether to proceed with a law enforcement investigation. If it is the first time a particular activity has been noted and it is of little significance, the data owner may decide that the resources are not available to support an investigation. If the emergency response team can relate the incident to other incidents, however, the team secures the system and reports its findings to law enforcement for further investigation.

2.4 PREPAREDNESS

Successful information assurance operations depend on information assurance preparedness. Preparedness activities range from development concepts and policies to resolution of legal authorities and regulatory responsibilities to the detailed technical implementation of these policies, authorities, and responsibilities. Since the last edition of this report, many significant coordination and development activities have begun. Some of the key activities are discussed in the following sections, which build on the previous editions of this report.

[65] CJCSI 6510.01B, *Defensive Information Operations*, page C-8.

SUMMARY

- Some operational concepts are beginning to converge in practice; e.g., incident reporting.
- A strategy for the operations aspects of information assurance is beginning to become evident, but will require additional input from the operating forces.
- Information assurance responsibilities are beginning to take shape, but require clarification in practice; e.g., exercises and war games.
- The operational environment is still not well defined — the private sector role is a continuing challenge.
- Intelligence support challenges remain to be addressed and resolved.
- Relationships with law enforcement agencies are being clarified.
- However,
  - Policy and doctrine are still incomplete.
  - Legal issues regarding monitoring remain.
  - Impact of deregulation in the telecommunications industry is still unknown.
  - The international aspects have really not been addressed at all.
  - The implications of emerging technology remain to be addressed.

SECTION 3

POLICY AND DOCTRINE

The purpose of this section is to review relevant National and DoD policy and doctrine initiatives, analyzing them for their potential implications. At both the national and DoD levels, several groups have developed or are developing policy or policy recommendations that may affect the DoD components. At both the national and DoD levels, the activities of these Advisory, Interagency, Study, and Working Groups are addressed first, followed by reviews of significant organizational policy and doctrine initiatives. The theme of convergence is also explored in the context of Service IO frameworks and in standardization efforts for operational terms.

CONTENTS

3.1 NATIONAL-LEVEL INITIATIVES

Advisory and interagency group roles may include a broad range of responsibilities; these responsibilities are not limited to developing policy or policy recommendations. Often the groups oversee processes and projects or recommend legislative and regulatory actions. However, the most likely near-term results of their activities will be mostly in the policy arena. For the Executive Branch, the Office of Management and Budget (OMB) has overall responsibility for Information Technology (IT) and IT security; therefore OMB's initiatives have significant bearing on DoD IA activities. Department of Commerce initiatives are also significant to OSD and the DoD components. The Department of Commerce is responsible for encryption export control and is the parent organization of National Institute of Standards and Technology (NIST), which is responsible for standards for the security of Federal unclassified information systems.

3.1.1 Advisory and Interagency Groups

President's Commission on Critical Infrastructure Protection

In response to Presidential Decision Directive 39, the Attorney General created a Critical Infrastructures Working Group to consider the vulnerabilities of and threats to eight critical infrastructures. The report of the Working Group recommended that a President's Commission be established to develop a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and to propose statutory and regulatory changes and to focus those efforts through consideration of eight specific infrastructures. The Commission was established by Executive Order 13010, *Critical Infrastructure Protection*, on

15 July 1996. Details of the Commission Membership and organization are found in Section 5.1.1.

The infrastructures being reviewed by the Commission include:

- **Telecommunications** — The networks and systems that support the transmission and exchange of electronic communications among and between end users (such as networked computers).
- **Electrical Power Systems** — The generation stations, transmission and distribution networks that create and supply electricity to end users so that end users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.
- **Gas and Oil Production, Storage and Transportation** — The holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels; the refining and processing facilities for these fuels; and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.
- **Banking and Finance** — The retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support entities that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.
- **Transportation** — The aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from a point-of-origin to a destination point in order to support and complete matters of commerce, government operations, and personal affairs.
- **Water Supply Systems** — The sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration and cleaning systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with wastewater and firefighting.
- **Emergency Services** — The medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to a public health or safety incident where speed and efficiency are necessary.
- **Continuity of Government Services** — Those operations and services of governments at federal, state, and local levels that are critical to the functioning of the nation's systems, i.e., public health, safety, and welfare.

Exhibit 3-1-1 shows the approach of the Commission.

Exhibit 3-1-1. PCCIP Approach for Developing Recommendations

Most of the nation's vital services are delivered by private companies. This reality creates a significant challenge in determining where responsibilities lie in protecting our critical infrastructures. The Commission is addressing that challenge by bringing the private and public sectors together to assess infrastructure vulnerabilities and to develop assurance strategies for the future. The Commission has consulted with security experts and engaged business executives from critical industries to collaborate in developing recommendations.

As part of its public outreach program, in early and mid-1997 the President's Commission on Critical Infrastructure Protection held five public meetings in different cities throughout the United States. At these meetings, scores of speakers had an opportunity to address comments and concerns about the infrastructures to the Commission.

In addition, the Commission has conducted research into the issues and sponsored games (discussed briefly in Section 2.3.4) to highlight the issues and provide insights into possible solutions. The report of the Commission is expected in October 1997.

The Commission is giving particular attention to issues that cut across the critical infrastructures. These include the following issues, as summarized from a recent Commission briefing: [66]

[66] President's Commission on Critical Infrastructure Protection, *Overview Briefing*, June 1997, observed on the Commission web page at http://www.pccip.gov/info.html on 1 August 1997.

- **Information Sharing in a Trusted Environment** — There is an obvious and compelling need to create a trusted and mutually beneficial environment for information sharing between the public and private sector. What is less obvious is *how* to create that trusted environment. The Commission will address mechanisms that could protect government source-sensitive intelligence information and private sector information affecting reputation, consumer confidence, and liability.
- **Risk Management** — Interdependency and complexity present new dimensions of risk, dimensions not fully reflected in the risk profiles used by infrastructures to guide investment decisions.
- **Economics** — Strengthening infrastructures will require increased investments, both public and private. The demand for a return on investment is driving the Commission to explore an array of investment incentives, regulatory changes, and use of standards.
- **Research and Development** — Modern technology is a large part of the problem, but also is an important part of the solution. The Commission is identifying infrastructure-related R&D throughout the government, academia, and industry. A review of the resulting data should result in an agenda for research and technology development specially focused on protection of the critical infrastructures.
- **Role of the Government** — The private sector must address protection against common-place intrusion, theft and fraud, but what about state-sponsored terrorism or hostile attack? What is the Federal government's responsibility? The Commission will attempt to define these respective responsibilities.
- **National Structures** — Given that the Federal government does have a role in infrastructure protection, current authorities and responsibilities provide the point of departure for effective analysis.
- **International Dimension** — In the contemporary political and business climate of trans-national market economies, global outsourcing of core functions, and multinational ownership of key infrastructure elements, secure operating standards and other rules are needed to promote reliably moving electronic information across borders.
- **Incentives for Private Sector Investment** — Should governments provide incentives for the private sector to invest in infrastructure protection? What will encourage companies to address vulnerabilities? How should incentives be structured?
- **Role of Insurance** — The Commission is exploring what role the insurance industry can and does play in achieving higher levels of infrastructure service delivery.
- **Assurance Safeguards** — The Commission also is exploring the role of standards in infrastructure protection. Should there be standards? Who should develop them? How should they be enforced?
- **Deregulation** — Deregulation of the power industry, for example, may have implications extending to other critical infrastructures.

- **Education and Awareness** — Many managers lack formal schooling in information technologies and are learning through on-the-job training. A younger population is fluent in information technology but less experienced in other aspects of business. We must adjust the educational system to close the gap.

The Commission will provide recommended legislative, regulatory, and policy initiatives for these and many other issues, including infrastructure specific issues. The Commission will also recommend organizations, public and private, to be responsible for implementation, and whether that implementation should be centralized or decentralized.

The Commission also is developing a recommendation for a follow-on organization and structure to guide implementation of the Commission's recommendations and provide continued attention to critical issues.

Finally, the Commission acknowledges that its members "are under no illusions that the Commission's recommendations can solve every aspect of every infrastructure problem." [67] Instead, the Commission sees its "strategy and recommendations as a point of departure for a continuing collaborative effort between government and the private sector." [68]

Moynihan Commission

On 30 April 1994, the President signed legislation appointing the Commission on Protecting and Reducing Government Secrecy. This legislation called for comprehensive reform to reduce the volume of classified information, strengthen the protection of legitimately classified information, and improve current procedures for granting security clearances. The Commission met for the first time on 10 January 1995, and consisted of 12 members: 4 Members of Congress, 1 senior Executive Branch official, and 7 people from the private sector. The Commission staff included specialists detailed from the Department of State, the Department of Defense, the Central Intelligence Agency, and the National Security Agency. The Commission published its final report on 3 March 1997.

The Commission staff investigated issues and solicited views from government officials, industry representatives, scientists, historians and archivists, journalists, and other interested parties on classification, declassification, and personnel security issues and on how new information technologies might affect the protection and reduction of secrecy for the rest of this decade and the 21st century. Exhibit 3-1-2 summarizes recommendations made by the Commission and transmitted to the President.

[67] Ibid.
[68] Ibid.

- To improve the functioning of the secrecy system and the implementation of established rules, we recommend a statute that sets forth the principles for what may be declared Secret.
- To enhance the understanding of classification and declassification decisions, we suggest adopting the concept of a life cycle for secrets.
- To improve declassification procedures, we recommend establishing a national declassification center to coordinate how information that no longer needs to be secret will be made available to the public; among its roles would be to declassify information using guidance from the agencies that originate the information.
- To promote greater accountability, we recommend establishing a single, independent Executive Branch office responsible for coordinating classification and declassification practice and enhancing incentives to improve such practice.
- To ensure that classification is used more efficiently, we recommend improving the initial classification of information by requiring classifying officials to weigh the costs and benefits of secrecy and to consider additional factors in the decision to make or keep something secret.
- To clarify the grounds for classifying intelligence information, we recommend that the Director of Central Intelligence issue a directive concerning the appropriate scope of sources and methods of protection as a rationale for secrecy.
- To promote the use of personnel security resources in a manner that ensures more effective and efficient protection, we recommend standardizing security clearance procedures and reallocating resources to those parts of the personnel security system that have proven most effective in determining who should or should not have access to classified information.
- To reduce the redundancies and costs of special access programs, we recommend measures to standardize security practices in such programs.
- ***To promote more awareness of the threats to automated information systems, we recommend steps to focus greater attention and promote increased cooperation on means for protecting such systems.***

Exhibit 3-1-2. Summary of the Recommendations of the Moynihan Commission

It should be noted that the final recommendation suggests increased awareness of and cooperation on the means for protecting automated information systems. It may be too early to predict what, if any, impact the Commission's effort may have. However, this is not the first group in recent history to study the classification system. The system has been subjected to six different executive orders since 1951; four in the last 25 years. There have been repeated adjustments (and, in some cases, major shifts in emphasis) without significant corresponding improvements in effectiveness of the classification system. All Commissioners agreed that dramatic transformations in the last 40 years necessitate a need to change the system for protecting government secrets in place today. Costs must be contained and new approaches are needed because of changing security threats and risks. While redundancies perhaps could be tolerated in the past, today's realities require much more efficient, prioritized, and cost-effective procedures.

National Security Telecommunications Advisory Committee (NSTAC)

The Information Assurance Task Force of the President's National Security Telecommunications Advisory Committee (NSTAC) recently completed two information assurance risk assessments. The assessment of the electric power industry concluded that compared to physical destruction, "electronic intrusion represents an emerging, but still relatively minor, threat." [69] However, the Task Force concluded that "downsizing, increased competition, and the shift to standard protocols will add to the potential sources of attacks, whether from inside, or outside, a utility." The assessment recommended several initiatives to the President and the electric power industry in the areas of awareness, information sharing, and mechanism for prevention and detection of and response to infrastructure disruptions. In reviewing the financial services information infrastructure, the Task Force found that "at the national level, the infrastructure is sufficiently protected and prepared to address a broad range of current threats, from natural disasters to electronic intrusions." [70] However, in light of the dependence on a telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from merger and acquisition, and the introduction of web-based banking services, this conclusion may be transitory. The financial services risk assessment recommended that the President assign an appropriate department or agency to identify mechanisms for sharing threat and risk mitigation information, to develop a solution for effective background investigation of personnel in sensitive positions, and to monitor the emergence of new banking and payment services. Finally, the Information Assurance Task Force is currently planning a combination seminar and exercise to arrive at a risk assessment of the transportation infrastructure.

In addition to these efforts, NSTAC working groups are addressing several information assurance issues from the national and private sector perspectives. These issues include:

- Assessing how to deal with widespread outages of the telecommunications infrastructure.
- Reviewing the state of intrusion detection practices, capabilities, and research and development in the telecommunications industry.
- Exploring private sector and government cooperation in addressing cyber-crime.

U.S. Security Policy Board (SPB) and the National Security Telecommunications and Information Systems Security Committee Information Assurance Document

Presidential Decision Directive 29 (PDD 29), *Security Policy Coordination*, dated 16 September 1994, [71] revised the security policy process on the basis of the greater diversity of threats to U.S. national security following the end of the Cold War. PDD 29 recognized a broader range of issues that affect national security, including economic issues and the proliferation of technologies from those used to create weapons of mass destruction to information technology.

---

[69] President's National Security Telecommunications Advisory Committee, Information Assurance Task Force *Electric Power Information Assurance Risk Assessment* (March 1997).

[70] President's National Security Telecommunications Advisory Committee, Information Assurance Task Force *Financial Services Risk Assessment Report* (August 1997).

[71] The President, Presidential Decision Directive (PDD) 29, *Security Policy Coordination* (16 September 1994).

PDD 29 created the United States Security Policy Board (SPB), which addresses a variety of security issues, including information systems security and risk management. The SPB considers policy directives for U.S. security policies, procedures, and practices. It recommends implementation of these directives to the President, through the Assistant to the President for National Security Affairs. The Policy Board coordinates the directives with all involved U.S. departments and agencies, ensuring affected parties are allowed to comment on such proposals. The SPB also coordinates the development of interagency agreements and resolves conflicts that may arise over the terms and implementation of these agreements.

Under the auspices of the SPB, an interagency working group developed a draft Information Systems Security Policy and Information Assurance Document or Manual, often referred to as the Information Assurance Document (IAD). The IAD is currently in coordination for possible release by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). The NSTISSC was created in 1990 by National Security Directive 42, though predecessor organizations date back much further. The NSTISSC's mission is to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of the Directive. The purview of the NSTISSC is limited to national security information and information systems. The SPB has generally limited its focus to national security information and information systems. This gives both groups oversight of classified national security information, as well as "Warner exempt" [72] information. The IAD, however, addresses only the protection of classified information. Limiting the scope of the IAD may have been a matter of simplification, as it can be difficult to address the assurance of both unclassified and classified information in the same policy and procedures document. The SPB/NSTISSC may also have limited the scope to classified information to ensure compliance with the letter and the spirit of the *Computer Security Act of 1987*, which granted to NIST purview of information systems security for systems processing unclassified federal information.

A leading approach to information assurance policy and procedures for interconnected systems, the IAD provides structure and guidance for a risk-management based approach to information systems security. It also breaks from Cold War security policy, which largely equated information security to confidentiality, by also addressing the integrity and availability requirements of information. An early draft of the IAD addressed roles and responsibilities, risk management, certification and accreditation, interconnected systems, administrative security requirements, and life-cycle security. It also and introduced Levels of Concern and Protection Levels. The purpose of the Levels of Concern and Protection Levels is to "level the playing field" on interconnected systems; e.g., to ensure similar levels of protection for similar information on interconnected systems. Exhibit 3-1-3 depicts the IAD concept relating these Levels of Concern and Protection Levels to required system security features and assurances.

---

[72] "Warner exempt" refers to information, as set forth in Title 10 U.S.C. Section 2315, that involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or equipment that is critical to the direct fulfillment of military or intelligence missions. The Warner Amendment excluded information systems and services associated with this information from some of the ADP procurement requirements of the Federal Property and Administrative Services Act of 1949.

The IAD provides information sensitivity matrices to help determine the appropriate Levels of Concern (High, Medium, or Low) for the Confidentiality, Integrity, and Availability for the information in a system. Protection Levels (1-6) are based upon the Level of Concern for Confidentiality, the clearances of personnel with access to the system, formal access approvals, and their need to know the information. The IAD then specifies Required System Security Features and Assurances for each Protection Level and for High, Medium, and Low Levels of Concern for Integrity and Availability.

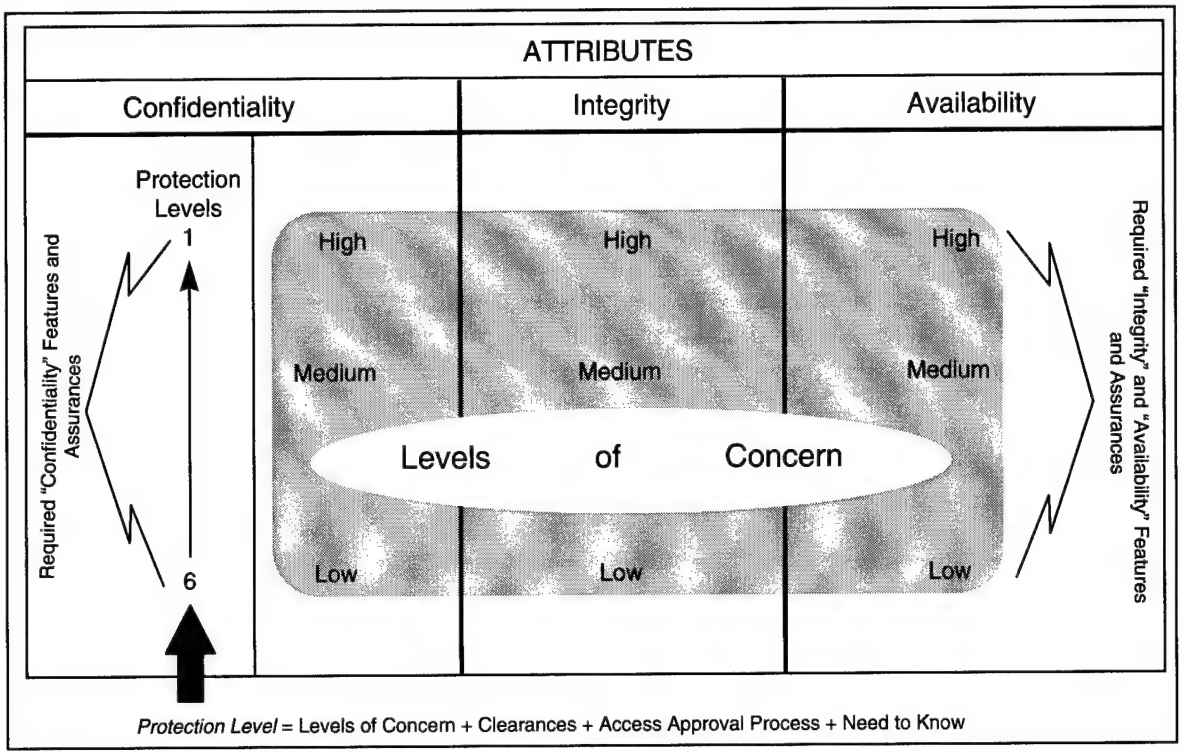


Exhibit 3-1-3. Information Sensitivity and Required System Security Features

The IAD approach reflects an effort to move from pure compliance-based security to a risk-management based approach. Although untested, it may represent a first step in an evolution from compliance to true risk management. Indisputably, the criticality of classified national security information merits a cautious approach to change. A similar approach to the assurance of sensitive unclassified information and information systems might be equally useful for ensuring comparable assurance for information on interconnected systems.

3.1.2 Office of Management and Budget

At the national level, Executive Office of the President policy initiatives include implementation of the *Government Performance and Results Act of 1993* (GPRA) and the *Information Technology Management Reform Act of 1996* (ITMRA). Continuing congressional interest has focused attention on agency strategic planning and the strategic Information Resource Management (IRM) plans required by the GPRA and the *Paperwork Reduction Act of 1995* (PRA). Agencies can also expect increased OMB oversight of their IT security activities; a 1996

General Accounting Office (GAO) [73] report recommends that OMB oversight be more proactive in identifying and promoting resolution of fundamental security program weaknesses. The GAO report includes a recommendation that OMB ensure that the CIO Council address security as a priority.

The purpose of the *Government Performance and Results Act* was to reform Federal program performance with a series of pilot projects in setting program goals, measuring program performance against these goals, and public reporting on progress. The *Act* requires agencies to submit strategic plans for program activities to OMB and Congress by 30 September 1997, and to establish objective, quantifiable, and measurable performance goals for program activities. OMB issued Transmittal Memorandum 69, *Preparation and Submission of Strategic Plans and Annual Performance Plans,* on 23 May 1997. [74] This memorandum revised OMB Circular A-11 to incorporate the GPRA strategic planning requirements.

The *Paperwork Reduction Act of 1995* requires agencies to develop 5-year plans for meeting agency IT needs and to designate a senior IRM official who reports directly to the agency head to carry out agency IRM responsibilities under the *Act*. OMB Circular A-130, *Management of Federal Information Resources*, [75] requires agencies to develop system security plans and include a summary of their security plans in the strategic IRM plans required by the *Act*.

The *Information Technology Management Reform Act of 1996*, renamed the *Clinger-Cohen Act*, expands upon the requirements of the *Paperwork Reduction Act*, requiring agencies to appoint Chief Information Officers (CIOs) and to use business process reengineering and performance measures to ensure effective IT procurement and implementation. Executive Order 13011, [76] *Federal Information Technology,* was issued on 17 July 1996 to implement the requirements of ITMRA. Section 5.1.1 discusses this Executive Order in detail.

Recent OMB memoranda address ITMRA implementation issues such as multiagency contracts, funding for interagency support of ITMRA implementation activities, and long-term IT investment strategy guidance. OMB Memorandum M-97-16, *Information Technology Architectures,* [77] links FY 1999 IT funding to agency development of information technology objective enterprise architectures. The memorandum adapts the five-component model from the NIST Special Publication 500-167, *Information Management Directions: The Integration Challenge.* [78] Technical Infrastructure, one of the components of the model, includes a requirement for a security standards profile that is consistent with the requirements of OMB Circular A-130. Security services such as identification, authentication non-repudiation, audit

---

[73] General Accounting Office (GAO), GAO/AIMD-96-110, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (September 1996).

[74] Executive Office of the President, OMB, Transmittal Memorandum 69, *Preparation and Submission of Strategic Plans and Annual Performance Plans* (23 May 1997).

[75] Executive Office of the President, OMB, Circular Number A-130, *Revised Management of Federal Information Resources* (8 February 1996).

[76] The President, Executive Order 13011, *Federal Information Technology* (17 July 1996).

[77] Executive Office of the President, OMB, Memorandum M-97-16 *Information Technology Architectures* (18 June 1997).

[78] Department of Commerce (DoC), National Institute of Standards and Technology (NIST), Special Publication (SP) 500-167 *Information Management Directions: The Integration Challenge* (September 1989).

trail creation and analysis, access controls, cryptography management, and virus prevention are called out in the Security Standards profile. This reflects a common theme of addressing security requirements as an integral part of IT management, architectures, and development. It also is interesting to note that the memorandum suggests the Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance Architecture Framework, Version 1.0, prepared by the C4I Integration Support Activity (CISA), as a published architectural model source.

From these policy initiatives, the statutory and policy requirements, and the general direction charted by Congress and the Executive Office of the President, several concepts with respect to IA can be inferred:

- Federal CIOs may be expected to play increasingly important roles in, and may be held responsible for, information assurance
- Agencies can expect increased pressure to develop strategic IRM plans that include summaries of their security plans
- Enterprise IT architectures that include security standards as an integral part of the architecture will be required
- Security plans, including strategic IRM plans, will be expected to embody performance measures.

3.1.3 Department of Commerce

The Department of Commerce is the parent organization of the National Institute of Standards and Technology (NIST). NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. NIST assists industry to develop technology to improve product quality, to modernize the manufacturing process, to ensure product reliability, and to facilitate rapid commercialization of products based on new scientific discoveries. *The Information Technology Management Reform Act of 1996* and the *Computer Security Act of 1987* assigned NIST the responsibility of developing government-wide computer system security standards and guidelines and security training programs for the protection of sensitive unclassified information maintained in Federal government computer systems.

NIST develops information system security guidelines, procedures, and technological solutions to help Federal agencies implement OMB policy. With a relatively limited budget and personnel strength, NIST must focus their efforts on issues with near-term impact and relevance to current policy initiatives. Current areas of interest include:

- Electronic commerce
- Public key encryption: infrastructure, certificate authorities, digital signatures, key recovery
- Common criteria for information technology security to replace the Orange Book trusted computer system evaluation criteria

- Advanced authentication
- Federal Computer Incident Response Capability (FedCIRC).

The first two topics are closely related. Without national and international standards for encryption and digital signatures, and a supporting public key infrastructure, progress in electronic commerce is limited. The Common Criteria recognizes the need to develop affordable alternatives to the Orange Book criteria, particularly for non-national-security information. The last two topics reflect NIST efforts to provide improved protection and response capabilities for the owners of federal information systems.

There has been significant encryption policy activity since the 2nd edition of this report was published on 4 July 1996. Much of this activity has been driven by public and private concerns over the security of the Internet and industry's desire for lifting the encryption export sanctions. Responsibility for export control of encryption was transferred from the Department of State (DoS) to the Department of Commerce (DoC). In October 1996, the Clinton Administration modified its stand on a key escrow policy, requiring escrow of encryption keys by a federal agency, and adopted a key recovery policy that relies on trusted parties (not necessarily government agencies) to verify digital signatures and to hold spare keys to confidential data. The executive order changing the policy allows the export of software utilizing 56-bit encryption keys if the company submits a plan for adding key recovery capabilities by January 1998. Encryption keys of any length are authorized for export provided an acceptable key recovery scheme is available. DoD, following the Administration lead, adopted a key recovery approach for FORTEZZA rather than the originally required private key escrow. Congressional efforts may render Administration policy invalid, if adequate votes can be mustered to pass current legislation and override a potential Presidential veto. Section 5 provides an in-depth discussion of recent encryption regulatory changes; Section 7 discusses encryption technology.

3.2 DEPARTMENT OF DEFENSE

Several key study groups have addressed information assurance issues. The recommendations of these groups will very likely influence DoD policy significantly. Working groups, normally made up of representatives of the DoD components, also have been chartered to address issues and develop policy, programmatic, and funding recommendations. The policy initiatives of these groups are addressed below, followed by a review of significant DoD component policy and doctrine initiatives.

3.2.1 Study and Working Groups

Quadrennial Defense Review

A QDR is required by the *Military Force Structure Review Act*, which was included as part of the *National Defense Authorization Act* for FY 1997. The Office of the Secretary of Defense conducts a QDR once every 4 years to assess long-term requirements and near-term strategies, thereby providing a blueprint for a strategy-based, balanced, and affordable defense program for the future.

In the realm of information operations, the 1997 report recognizes efforts under way to exploit information technology to adapt and transform the U.S. military. In stating that our current capabilities are adequate to defend against existing information operations threats, it does not overlook the fact that "the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century." [79]

In the context of *Joint Vision 2010*, the Department committed to:

- Develop additional guidance to bolster information assurance
- Allocate adequate resources for IA efforts within information technology investment programs
- Improve the Defense-wide planning and implementation process
- Regularly assess funding adequacies for all IA program components.

Defense Science Board Task Force on Information Warfare - Defense

To address some of the Defense Information Infrastructure protection issues, the Undersecretary of Defense for Acquisition and Technology formed a Defense Science Board Task Force on Information Warfare (Defense) to "focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence." [80] The Task Force noted an "increasing dependency on the Defense Information Infrastructure and increasing doctrinal assumptions regarding the continued availability of that infrastructure" and indicated, "This dependency and these assumptions are ingredients in a recipe for a national security disaster." [81]

Following a fairly extensive discussion of the environment (growing dependencies on information and infrastructures, the nature of information warfare and infrastructures, vulnerabilities, and threats), the Task Force observed that:

- The threat posed by information warfare is not limited to the realm of national defense, and the effort to control the problem must encompass broader national security interests, including Congress, the civil agencies, regulatory bodies, law enforcement, the Intelligence Community, and the private sector.
- Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-networked systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries in cyberspace offers further anonymity. Information warfare is also relatively cheap to wage as compared to conventional warfare, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous.

---

[79] DoD, *Report of the Quadrennial Defense Review* (May 1997).
[80] DoD, Undersecretary of Defense for Acquisition and Technology (USD(A&T)) Memorandum for the Chairman, Defense Science Board (4 October 1995).
[81] Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare - Defense.*

- Information warfare has been particularly troublesome for the Intelligence Community because IW is a non-traditional intelligence problem. It is not easily discernible by traditional intelligence methods. Formerly, capabilities were derived from unique observables and indicators of military capability open to our sensors, amenable to cataloging in databases, and understandable by classic analytic techniques.
- The reality of limited resources has fostered the current acquisition practice of trading off functionality, performance, and numbers of systems delivered to the operating forces at the expense of security. On a positive note, recent policy updates clearly state the need for attention to the information warfare aspects of systems acquisition.
- The concept of protecting large portions of the information infrastructure is not valid. It is economically and technically impossible to close every possible vulnerability. We need to focus on designing a resilient and repairable information infrastructure.
- We need to focus on establishing information domains within the information infrastructure, which will minimize cascading effects and enable us to contain the battle damage resulting from an information warfare attack.
- Market forces are extremely powerful, but will not alone provide the capability desired. The market simply does not perceive the possibility of a strategic information warfare attack against information centers of gravity. The market is not sufficiently informed about the vulnerabilities and threat to make rational national security judgments.

The Task Force made over 60 specific recommendations regarding the increasing dependency and doctrinal assumptions. These specific recommendations were categorized under the key recommendations shown in Exhibit 3-2-1.

Bottom Line — DoD has an urgent need to:

1. *Designate an accountable IW focal point*
2. *Organize for IW-D*
3. *Increase awareness*
4. *Assess infrastructure dependencies and vulnerabilities*
5. *Define threat conditions and responses*
6. *Assess IW-D readiness*
7. *"Raise the bar" (with high-payoff, low-cost items)*
8. *Establish a minimum essential information infrastructure*
9. *Focus the R&D*
10. *Staff for success*
11. *Resolve the legal issues*
12. *Participate fully in critical infrastructure protection*
13. *Provide the resources*

DSB has been urging action on this problem for 3 years!

Exhibit 3-2-1. DSB Task Force Recommendations

The Task Force reviewed all of the individual recommendations categorized under the key recommendations above and estimated to $5 million granularity what the implementation costs might be. The total estimated cost for the recommendations was $3.01 billion. These estimates were in addition to the current Information Systems Security Program and other distributed information security costs, which in the aggregate total about $1.6 billion annually.

The Department has undertaken many initiatives in response to the Task Force recommendations. A few examples include:

- Establishing a Global Operations and Security Center (GOSC) within DISA to monitor the operational and security posture of the DII.
- Developing concepts for Red Teams and conducting seminars and conferences to address associated issues.
- "Raising the bar" by directing use of digital signatures based on Federal Information Processing Standard 186.
- Establishing a Critical Infrastructure Protection Working Group to aid the Joint Program Office for Special Technical Countermeasures in assessing dependencies on critical infrastructures.
- Developing information threat conditions and appropriate responses.
- Conducting realistic cyber-war exercises.
- Working for certification of operators and systems administrators.
- Establishing a career path for systems administrators (civilian and military).

While much remains to be done, the Task Force report, in conjunction with the results of some of the initiatives, has succeeded in generating considerable interest, attention, and activity related to information assurance.

Information Assurance Task Force

Program Decision Memorandum II, dated 9 October 1996, required that the ASD(C3I) provide to the Deputy Secretary of Defense an assessment of the Services and Defense Agency information assurance programs, a comparison of information assurance plans with programmed resources, and an evaluation of projected program performance. In response, the ASD(C3I) directed the Director, National Security Agency, to establish an Information Assurance Task Force to conduct the assessment, comparison, and evaluation. The resulting report "provides a general assessment of the Department's current IA posture and a comprehensive approach to achieving an integrated IA program." [82] As a part of its activities, the Task Force developed an information assurance process model — an operational process that continuously integrates people, policies, technology, procedures, and doctrine.

---

[82] DoD, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASDC3I), *Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense* (28 March 1997).

Critical Infrastructure Protection Working Group

The Critical Infrastructure Protection Working Group (CIPWG) is identifying coordinating mechanisms and developing a common and formalized process among the DoD Components for the protection and assurance of DoD and non-DoD critical infrastructures — both national and international. Chaired by OUSD(P) and OADS(C3I), with OUSD(P) Infrastructure Policy Directorate serving as Executive Secretary, the CIPWG serves two primary functions: interface between DoD and the PCCIP, and review and assess DoD infrastructures. The multi-year effort is focused on eight critical DoD infrastructures whose integrity, availability, survivability, and capability is considered essential for fully integrated support to DoD operations including National Security and Emergency Preparedness (NS/EP) missions. Exhibit 3-2-2 depicts the challenges of such an effort in "closing the gap" of interdependencies.

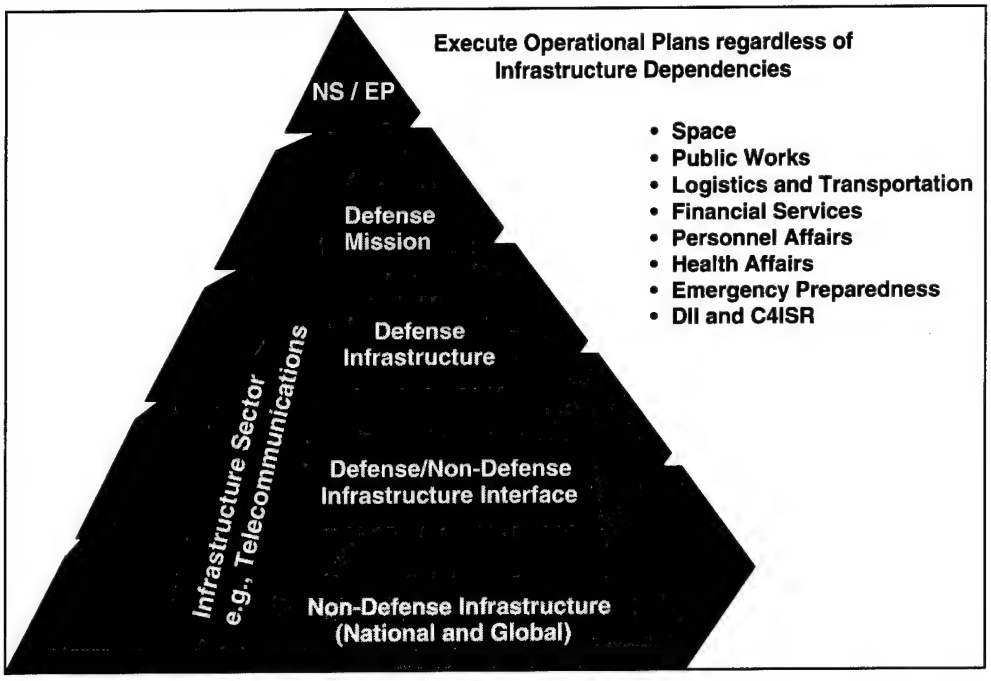


Exhibit 3-2-2. "Closing the Gap" on Critical Infrastructures and Industries Supporting National Security and Emergency Preparedness Objectives

Information Assurance Group (IAG)

To enhance cross-Service and Agency coordination on defensive information operations preparedness activities, the Office of the Assistant Secretary of Defense (C3I) has established the Information Assurance Group (IAG), chaired by a representative from the OASD(C3I) and consisting of representatives from the Joint Staff, Services, and Agencies (DIA, NSA, DISA, etc.). The IAG establishes priorities and provides guidance and oversight for its many working groups. Members of these working groups generally include Joint Staff, Service, and Agency representatives with experience and responsibilities in the working group functional areas. CINC representatives belong to key groups. The IAG and subordinate working groups are playing a key role in helping DoD address priority IA issues and coordinating Component initiatives.

Updating DoD policy is a major focus area of these groups. The following paragraphs provide an overview of these working groups, their focus, and current activities.

- **IA Policy Working Group (IAPWG)** — Co-chaired by NSA and DISA, the IAPWG is chartered to pull together the policy-making activities of the other working groups and to develop a DoD IA Policy Directive and an implementing manual to update the 1988 DoD Directive 5200.28, *Security Requirements for ADP Systems*. The IAPWG has a draft IA Policy Directive which is currently being reviewed by the IAG. Formal coordination is targeted for October 1997. An on-line IA policy resource environment is envisioned to promote greater access, information sharing, and to facilitate update.

- **Joint IA Tools Working Group** — The IA Tools WG is chartered to coordinate implementation of DoD IA tools. This working group leverages the activities of the CINCs, Services and Agencies (C/S/A), national labs and others, and coordinates activities with other working groups. Currently, it is coordinating the efforts of a Navy-led development of a Joint Incident Handling and Vulnerabilities Database with the Joint IA Operations Working Group and is coordinating tool distribution policy with the IAPWG. It sponsored a recent flyoff, conducted by the Navy and MITRE, of commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) intrusion detection tools to determine the maturity of the products and whether any met critical DoD requirements. Preliminary conclusions indicate that both COTS and GOTS must be developed further to meet requirements. The Tools Working Group also gives the C/S/As an opportunity to provide feedback on the DISA Tool Program Management Plan. They also are working to modify the rule set of a CIA automated risk assessment tool to provide automated support for the DITSCAP process.

- **Joint IA Operations Working Group (JIWG)** — The JIWG was established to develop and implement an integrated IA response capability. Key goals include integrating and coordinating computer IRT operational procedures and incident detection and reporting, as well as coordinating event responses. Key to this effort is standardization of terminology. Membership includes the DISA ASSIST, OMNCS, NSA, Service, and CINC computer IRTs (including the Coast Guard) and the FBI CITAC as well as advisors including Joint Staff representatives, DIA, OASD(C3I), NCIS, and CIAC. The JIWG has baselined more than 20 operational terms. If approved, these terms and definitions will be promulgated in DoD policy, Joint Staff policy and doctrine, and the NSTISSC glossary. The JIWG also is addressing common event assessment and incident handling procedures, warning dissemination through IRTs and command channels, common formats for reporting and warnings, thresholds for reporting, common equipment suites, common incident response training requirements, and InfoThreatCons.

- **Multilevel Security Working Group (MLS WG)** — The MLS WG has been in existence since 1990, but was only recently brought under the auspices of the IAG. A draft charter is in coordination. The MLS WG has provided a proposed data labeling policy to the IAPWG and plans to develop a MLS Project Managers' Handbook.

- **Secret and Below Interoperability Working Group (SABI WG)** — The objective of the SABI WG is to develop a process for SABI implementations. The SABI WG maintains NIPRNET and SIPRNET web pages and a listing of SABI Reference

Implementations that describes historical SABI implementations. Other activities include developing a Joint Schedule of Implementations, which is an effort to leverage and coordinate System Security Engineering Support resources. The SABI WG also is defining Maximum Acceptable Risk Levels for SABI connectivity. An approved Maximum Acceptable Risk Level will ensure that decisions made by a single DAA do not present unacceptable risk to other interconnected networks and systems. Once coordinated and approved, the Maximum Acceptable Risk Level will reflect the community's judgment of acceptable risk. The SABI WG envisions updating the Acceptable Risk Levels every 6 months. A Joint Vulnerability Assessment process also is being pursued to validate that SABI implementations meet and maintain required safeguards.

- **Education, Training, Awareness, and Professionalization Working Group (ETAPWG)** — The ETAPWG was chartered to address IA/INFOSEC education training, awareness, and professionalization issues on behalf of ASD(C3I). Membership includes C/S/A education, training, and awareness (ETA) providers and program managers. ETAPWG objectives include identifying gaps in instruction, recommending and developing solutions, assigning lead organizations for initiatives, eliminating duplication of effort, and standardizing instruction content. Initiatives are focused on one of four levels identified by NIST: awareness, literacy, training, and education. The ETAPWG has a draft DoD Directive in informal coordination and will develop input for a DoD IA Policy Directive.
- **Certification and Accreditation Working Group (C&A WG)** — A recently established working group under the IAG, the C&A WG can capitalize on the groundwork under way at DISA in the areas of Certification and Accreditation (C&A) and DII Connection Approval Program (CAP). It is expected that the working group will coordinate implementation and updates of the DoD IT Security Certification and Accreditation Process (DITSCAP) and develop formal connection approval requirements. C&A and CAP are related, though distinctly different, critical functions.
  - **Certification and Accreditation** — One of the key elements of ensuring a protected information environment is having responsible individuals certify that systems designated for processing classified information are operated in accordance with agreed upon standards. DISA revised the DITSCAP and it is expected to be signed out during the third quarter of FY 1997. DISA expects to publish a C&A Process Handbook for Certifiers in the near term. The DITSCAP establishes the standard process for C&A of IT, including automated information systems and networks within the DoD. The process consists of four phases. [83]
    - > **Phase I, Definition**. The Definition Phase documents the system mission, environment, and architecture; defines the levels of effort; identifies the DAA; and documents the security requirements. Phase I culminates with an

[83] DoD Instruction (Draft), *DoD IT Security Certification and Accreditation Process (DITSCAP)* (12 May 1997). On Internet at http://mattche.iiie.disa.mil/ditscap/DODI_total.html

agreement of the approach between the Program Manager, DAA, and the User Representative.

> **Phase II, Verification**. The Verification phase verifies the system's compliance with previously agreed security requirements. For each life-cycle development activity, there is a corresponding set of security analysis activities to verify compliance with the security requirements and evaluate vulnerabilities.

> **Phase III, Validation.** The Validation Phase evaluates the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation culminates in an approval to operate.

> **Phase IV, Post Accreditation.** The Post Accreditation Phase monitors system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, and periodic compliance validation reviews are conducted.

– **DII Connection Approval** — CJCS Instruction 6211.02 details policy and delineates responsibilities for life-cycle management of DISN and connected systems. Each DoD system or application device having a requirement for long-haul common-user information transfer services is to be identified for planning purposes by DoD activities. The Chairman of the Joint Chiefs of Staff, Chiefs of Services, CINCs, directors of Defense agencies, or designated representatives validate operational requirements and certify them before requesting connection approval. DISA provides approval for DISN connections, ensuring all technical and interoperability requirements are met and that subnetworks, systems, and other connected components provide adequate security and have been properly accredited. DISA is currently implementing a connection approval process for the Secret Internet Protocol Routing Network (SIPRNET) and is planning a similar process for the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET). A SIPRNET Connection Security Requirements document is in final draft. DISA has granted connection approval for more than 260 of the more than 352 SIPRNET connections.

3.2.2 Office of the Secretary of Defense (OSD)

In December 1996, following an extensive coordination effort, Deputy Secretary of Defense White signed out DoD Directive S-3600.1, *Information Operations*. The new directive reflects a framework that had evolved since the publication of the predecessor directive in 1992. The terminology associated with this new framework was introduced in Section 1.3, Background. Since its publication, OSD and other DoD Components have sought to induce a culture change within DoD embracing the new framework. To aid in understanding the challenges, OSD sponsored several study and working groups to help identify the issues, evaluate alternatives, and recommend actions. The groups, described in Section 3.2.1, Study and Working Groups, have already influenced DoD policy.

Emerging Policy on Infrastructure Protection

Several study groups recognized quickly that infrastructure protection — including the protection of the information components of other infrastructures — was equally important to IA and military operations. In response to this realization, the USD(P) developed a draft infrastructure protection policy in coordination with the Critical Infrastructure Protection Working Group and OASD(C3I). Their efforts include a draft Critical Asset Assurance Program (CAAP) directive, which is currently in coordination. The purpose is to "identify and ensure the availability, integrity, survivability and adequacy of those assets (domestic and foreign) whose capabilities are deemed critical to DoD Force Readiness and Operations in peace, crisis, and war by providing for their protection from all hazards; mitigating the effect of their loss or disruption; and planning for timely restoral or recovery. Critical Assets include information systems and computer based systems and networks that can be distributed in nature." [84] This fairly comprehensive draft policy statement incorporates many of the recommendations made in the recent past regarding information and infrastructure assurance. For example, it directs the heads of DoD Components to include a contractual requirement of cooperation in vulnerability assessments and assurance planning when contracting for private sector facilities, services, and products and to consider all-hazard assurance of service when awarding contracts. It also institutionalizes many of the activities of the Critical Infrastructure Protection Working Group. The CAAP draft policy includes, among others, the following elements:

- Establishes DoD policy to identify and ensure the availability, integrity, survivability, and adequacy of those assets (domestic and foreign) whose capabilities are deemed critical to DoD Force Readiness and Operations in peace, crisis, and war by providing for their protection from all hazards, mitigating the effects of their loss or disruption and planning for timely restoral or recovery.
- Recognizes that Critical Assets include information systems and computer-based systems and networks that can be distributed in nature.
- Designates the Secretary of the Army as the Executive Agent for the Program.
- Directs assessments of infrastructure dependencies and vulnerabilities.
- Requires the Director of Defense Investigative Service (DIS) to develop on-site survey procedures, conduct on-site surveys and vulnerability analyses of physical and technical threats to designated assets, etc.
- Directs ASD(C3I) to coordinate with the NCS to identify critical NII assets and provide overall coordination of computer incident response activities.
- Directs SECNAV to provide infrastructure assurance analysis through the Joint Program Office for Special Technical Countermeasures (JPO-STC).
- Directs heads of DoD components to include a contractual requirement for cooperation in vulnerability assessments and assurance planning in contracts for private sector facilities, services, and products.

---

[84] DoD, DoDD 5160.54 *Critical Asset Assurance Program*, Draft (6 June 1997).

3.2.3 Joint Staff

The Chairman, Joint Chiefs of Staff, published three key documents relevant to IO/IA since the 2nd edition of this report. Taken together, these documents provide a holistic view of IO. They provide guidance for developing future capabilities [85] and a current baseline of policy [86] with emphasis on the day-to-day IA requirements and doctrine [87] addressing IO in joint warfighting.

Published in May 1997, the *Concept for Future Joint Operations* is intended to be the first step in an implementation process designed to transform the operational concepts of *JV2010* into joint doctrine and operational procedures. The CFJO proposes an implementation process that takes advantage of existing processes to assess alternatives and develop new approved capabilities. The scope of *CFJO* is far broader than IO/IA but *CFJO* recognizes that Information Superiority, and the underlying technological innovations, are the enabler of the four objective operational capabilities. It also addresses IO in some depth.
From an IA perspective, *CFJO* recognizes that terrorist attacks on information systems are likely to increase as the attack tools become more prevalent and as increased antiterrorist efforts make physical attacks less likely to be successful. It also addresses several concepts that are not easily answered and merit greater study. The inclusion of these concepts in this first version of *CFJO* is encouraging and reflects a willingness to begin to address these ***"tough nuts."*** Exhibit 3-2-3 identifies some of these IA issues as extracted from *CFJO*.

- We need to understand the potential significance of our reliance on technological solutions alone.
- Information processing system capabilities can cause data overload.
- The concept of information superiority in JV 2010 does not imply perfect intelligence.
- Sophisticated information systems can fail.

Exhibit 3-2-3. "Tough Nuts"

The Chairman, Joint Chiefs of Staff, also published CJCS Instruction 6510.01B, *Defensive Information Operations*, on 22 August 1997. The revision cancels CJCSI 6510.01A and reflects the Joint Staff evolving IO doctrine, adopts the DoDD S-3600.1 framework and incorporates new operational policies. CJCSI 6510.01B provides implementing guidance and supplemental joint policy for defensive information operations. CJCS specific policy guidance requires that information, information-based processes, and information systems (such as command, control, communications, and computers [C4] systems, weapon systems, and infrastructure systems, etc.) used by U.S. military forces will be protected relative to the value of the information contained therein and the risks associated with the compromise of or loss of access to the information. Enclosures to the CJCSI describe a process, procedures, and responsibilities for defensive information operations. Significant to this revision is strengthening the requirement for reporting

[85] *Concept for Future Joint Operations* (CFJO).
[86] CJCSI 6510.01B, *Defensive Information Operation.*
[87] Joint Pub 3-13, *Joint Doctrine for Information Operations*, Draft.

incidents involving non-national security systems. DISA, in coordination with NSA and the Joint Staff, is charged with developing policy and procedures for ensuring that all incidents are reported through appropriate channels.

A revision of Joint Pub 3-13, entitled *Joint Doctrine for Information Operations*, is currently in coordination. The concepts and processes are not entirely unique to the document; rather, they ensue from the continuing convergence of DoD IO doctrine and policy, which, to some extent, is reflective of the dynamic interagency coordination of IO initiatives. Joint Pub 3-13 provides a common framework within which the C/S/As can incorporate IO across the spectrum of day-to-day to wartime activities. Guidance includes processes and principals for joint IO and organizational planning guidance. Particularly noteworthy is the guidance for incorporating IO into training and exercises and the increased emphasis on integration of offensive and defensive IO.

3.2.4 Services

The Military Departments continued to develop concepts and guidance to implement the principles of *JV2010* in the area of information operations and protection of information.

The Army's *Army Vision 2010* [88] emphasizes that IO conducted to gain *information dominance* (a degree of information superiority) are essential to all operations. They consist of both offensive and defensive efforts to create a disparity between friendly and enemy knowledge of the battlespace. Field Manual 100-6 *Information Operations*, [89] released in August 1996, contains the Army view that the then-current joint doctrine understanding of Information Warfare (IW) was too narrowly focused on actual conflict, rather than on the full range of military operations. IO are defined as continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. IO include interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities. The three interrelated components of IO are: operations, relevant information and intelligence (RII), and information systems (INFOSYS). The protection of C2 capabilities (C2-protect) is one of two branches of C2W (command and control warfare — a warfighting application of IW). The first critical step in protecting IO capabilities is to identify specific and potential threats against targets identified and prioritized in terms of criticality and vulnerability. Because everything cannot be protected, risk management analysis identifies essential information and INFOSYS that must be kept free from disruption or corruption. Offensive C2-protect uses the five elements of C2W to reduce the adversary's ability to conduct C2-attack. Defensive C2-protect employs physical, electronic, and intelligence protection. The Army's new brochure *Information Operations* (1997) is drawn from the new Field Manual 100-6. It emphasizes that improving C2-protect capabilities is the near-term priority in the effort to improve IO with training as the most important component.

---

[88] Department of the Army, *Army Vision 2010* (undated), available on Army Internet site at http://www.army.mil/2010/

[89] Department of the Army Field Manual (FM) 100-6 *Information Operations* (August 1996).

The Air Force's *Global Engagement: A Vision for the 21st Century Air Force* [90] identifies Information Superiority as one of its core competencies alongside Air and Space Superiority, Global Attack, Rapid Global Mobility, Precision Engagement, and Agile Combat Support. In this document, the Air Force commits to "aggressively expand its efforts in defensive IW as it continues to develop its offensive IW capabilities. The top IW priority is to defend our own increasingly information-intensive capabilities."

Already dedicated and operational in the garrison defense of computer systems, the Air Force will continue to invest in defensive IW, and move to defend its forward-deployed assets, particularly in Battle Management/Command and Control (BM/C2). In *The 1997 Air Force Long-Range Plan: Summary*, [91] the Service re-affirms it will aggressively expand its efforts in defensive IO toward the goal of robust information protection for all Air Force assets, especially forward-deployed operational and tactical. It commits to develop IO capabilities in concert with other Services and defense and national agencies and organizations. Several new directives and instructions are notable. Air Force Policy Directive (AFPD) 31-4 *Information Security* (1 August 1997) [92] replaced the previous version of March 1995. Also, Air Force Policy Directive (AFPD) 33-2 *Information Protection* (1 December 1996) [93] superseded AFPD 33-2 *C4 Systems Security* (13 August 1993). The new directive requires training of systems users; system protection at a level commensurate with the risk and the magnitude of harm that could result from disclosure, loss, misuse, alteration, or destruction of the information or systems; certification and accreditation; and emphasis on information protection during acquisition. Air Force Systems Security Instruction 5021 *Vulnerability And Incident Reporting* (15 August 1996) provides guidance, procedures, and formats to develop vulnerability and incident reporting requirements for Automated Information Systems (AIS). Air Force Instruction (AFI) 10-1101, *Operations Security* (1 May 1997), [94] outlines the OPSEC process and program and emphasizes that "OPSEC is an integrated component of IW [that] provides a means of detecting and controlling an adversary's actions on our military information functions. OPSEC assists in protecting IW capabilities and intentions from adversary knowledge and attack."

Navy efforts on information protection policy and doctrine also progress. The Deputy Chief of Naval Operations (Plans, Policy, and Operations) (N3/N5) intends to establish a Strategic Policy Planning Cell to develop and coordinate OPNAV policy in the area of Information Warfare. The Navy continues to develop IW/C2W doctrine to be promulgated in the Naval Warfare Pub 3-13 series. Two works in progress are the Naval Warfare Publication 3-13.1, *Naval C2W*, and Naval Warfare Publication 3-13.1.1, *Navy IW/C2W Commanders Manual*. A new Secretary of the

---

[90] Department of the Air Force, *Global Engagement: A Vision for the 21st Century Air Force*. Available on Air Force Internet site at http://www.xp.hq.af.mil/xpx/21/nuvis.htm

[91] Department of the Air Force, *The 1997 Air Force Long Range Plan: Summary*. Available on Air Force Internet site at http://www.xp.hq.af.mil/xpx/7frame.htm

[92] Department of the Air Force, Air Force Policy Directive (AFPD) 31-4 *Information Security* (1 August 1997) available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

[93] Department of the Air Force, Air Force Policy Directive (AFPD) 33-2 *Information Protection* (1 December 1996) available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

[94] Department of the Air Force, Air Force Instruction (AFI) 10-1101 *Operations Security* (1 May 1997) available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

Navy Instruction SECNAVINST 3430.27, *U.S. Naval Computer Network Incident Response*, [95] is in draft preparation. Its purpose is to establish requirements , procedures, and appropriate formats for detecting, responding to, and reporting computer incidents. It will require all commands, units, and activities to report any actual or suspected computer intrusion incident to the Fleet Information Warfare Center. Also, a new OPNAVNOTE on information systems security is being developed to replace OPNAVINST 5239.1A.

Marine Corps Doctrinal Publication (MCDP) 6 *Command and Control* was issued in October 1996. [96] It provides a basis for development of C2 doctrine and other measures (e.g., tactics, techniques, procedures). Situational uncertainty is a fact and is dealt with by "mission command and control," which uses broad guidance rather than detailed directions, and communication as the basis for cooperation and coordination. All channels and methods should provide rapid, distributed, unconstrained flow of information in all directions, in the form of meaningful images discriminated in terms of importance, quality, and timeliness. A judicious combination of broadcast and point-to-point transmission and supply-pull and demand-pull should be used.

3.2.5 Contrasting Service Frameworks

Section 1.3 suggests that across DoD, the concepts and frameworks for Information Operations are converging. The extensive coordination process for DoD Directive S-3600.1 ensures, to a certain extent, a top-level approach and lexicon that was acceptable to the C/S/As. As the Services incorporated IO into their policy and doctrine and tactics, techniques and procedures, there was a need to "fit" IO into their overall roles, missions, and doctrine and describe it in terms that can be readily understood by Service members. Service implementations of IO also often preceded authoritative OSD or Joint Staff guidance. While in general compliance with DoD policy and joint doctrine, Service implementations often reflect different interpretations of the similar concepts and terms.

Exhibit 3-2-4 is an Air Force view of these variances.

> "Each service has its own unique operational demands....In developing the doctrinal constructs in this paper, we used airpower terminology and examples. That is our background, those are the terms and the environment with which we are familiar. But the argument we present **is not** dependent on terminology. Replacing Air Force terms with Army or Navy terms would leave the conclusions unchanged."
>
> *Cornerstones of Information Warfare,* August 1995

Exhibit 3-2-4. Cornerstones of Information Warfare

Exhibit 3-2-5 compares and contrasts a few of these concepts. The purpose is not to highlight the difference, but to contribute to the understanding of the domain and the doctrine of the participants.

---

[95] Department of the Navy, Secretary of the Navy Instruction SECNAVINST 3430.27 *U.S. Naval Computer Network Incident Response,*(Draft). Copy provided by Dept. of Navy staff.
[96] USMC, Marine Corps Doctrinal Publication (MCDP) 6 *Command and Control* (October 1996).

Term	OSD	Army	Navy/ USMC	Air Force
Information Dominance	Not found in OSD publications	A degree of information superiority		Not found in doctrinal publications
Information Superiority	The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same	Not found in doctrinal publications	The Navy generally follows OSD terminology.	One of six core competencies
C2-Protect	Not found in OSD publications	Maintenance of effective C2 of own forces; minimizing friendly vulnerabilities; transcends range of military operations		Not found in doctrinal publications
Information Operations	Actions taken to affect adversary information and information systems while defending one's own information and information systems.	Continuous military operations within the Information Environment; composed of relevant information and intelligence, information systems, and operations		Ascribes to the OSD definition
Information Assurance	Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.	Not found in doctrinal publications		Information protection is in common use
Information Protection	Not found in OSD publications	Not found in doctrinal publications		Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of systems and information. [Similar to DoD Directive S-3600.1 definition for Information Assurance]
Counter-information	Not found in OSD publications	Not found in doctrinal publications		Actions dedicated to controlling the information realm

Exhibit 3-2-5. Service Doctrine

3.2.6 Urgency of Standardized Operational Terms

While there is some room for divergence — and continuing dialog — of evolving IO concepts, strategy, and lexicons, there is also a recognized need for the common use and understanding of operational terms at the tactical and the national level. A common understanding of "tactical" terms, such as event, incident, intrusion, indicator, probe, and vulnerability, is critical in the context of incident and vulnerability information sharing and reporting. It is equally important at the national level for agencies to have a common understanding of the definitions and associated legal authorities and bounds indicated by another set of operational terms. This set includes such terms as clandestine operations, Presidential Approval, covert action, etc. This discussion is incorporated in this section, because standardized terminology is often developed by policymaking forums and the approved terms are often documented in policy documents.

The Joint Information Assurance Operations Working Group, composed of representatives from CINC, Service, DoD, and Federal Agency emergency response teams and organizations with similar responsibilities and interests, is working to standardize terminology, particularly those terms necessary for reporting and sharing information on computer incidents. Exhibit 3-2-6 is a list of selected terms and working definitions. Other JIWG proposed terms and definitions can be found in Appendix C, Glossary. Where possible, the JIWG has adopted or modified definitions already in common use. It is expected that the results of the JIWG's efforts will be incorporated into OSD and/or CJCS policy documents and official glossaries.

Attack: The intentional act of attempting to bypass security controls on an Automated Information System.

Computer Intrusion: An incident of unauthorized access to data or an Automated Information System.

Correlation: The process which associates and combines data on a single entity or subject from independent observations, in order to improve the reliability or credibility of the information.

Event: Any suspicious pre-assessed activity.

Incident: An assessed event of attempted entry, unauthorized entry, and/or an information attack on a AIS. It includes unauthorized probing, browsing; disruption, or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent (e.g., malicious logic).

Indicator: An action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an aggressive act.

Malicious Logic: Hardware, software, or firmware that is intentionally included into an information system for an unauthorized purpose (e.g., virus and Trojan horse).

Threat: Any circumstance or event with the potential to cause harm to an AIS in the form of destruction, disclosure, modification of data, or denial of service.

Exhibit 3-2-6. JIWG Proposed Common Terminology

At the national level, a set of clearly understood operational terms and definitions also is critical. These terms are defined by U.S. Code, executive order, national security directives, or official glossaries and are integral to an approval process for covert actions. Though these terms were in existence long before the advent of Information Operations and are applicable to covert actions outside the scope of IO/IA, they bear new meaning to those in the Information Operations and Information Assurance community. In the current information environment, with tools and connectivity currently available, it is entirely possible that impromptu response by DoD personnel—albeit well intentioned—to malicious network or system probes or intrusions could easily exceed the authority of those involved; violate state, Federal, and international law and custom; and be perceived by some in the international community as aggressive or intelligence-gathering activities. It is important that DoD IO personnel ensure that appropriate approvals are obtained if IO are expected to deviate from traditional military activities. Exhibit 3-2-7 contains extracts of selected definitions and the location of the complete and official definitions.

Approval (Presidential; of covert action): The President may not authorize the conduct of a covert action by departments, agencies, or entities of the U.S. Government unless the President determines such an action is necessary to support identifiable foreign policy objectives of the U.S. and is important to the national security of the U.S., which determination shall be set forth in a finding that shall meet each of the following conditions:

(1) Each finding shall be in writing, unless immediate action by the U.S. is required and time does not permit the preparation of a written finding, in which case a written report of the president's decision shall be contemporaneously made and shall be reduced to a written finding a soon as possible, but in no event more than 48 hours after the decision is made.

(2) Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, that has already occurred.

(3) ...

(4) ...

(5) A finding may not authorize any action that would violate the Constitution or any statute of the U.S.. [USC 50 § 413]

Clandestine Operation: An operation sponsored or conducted by governmental departments or agencies in such a way as to ensure secrecy or concealment. ...[Joint Pub 1-02, March 94]

Covert Action: An operation that is so planned and executed as to conceal the identity or permit plausible denial by the sponsor. ... [USC 50 § 413b]

Exhibit 3-2-7. National Level Operational Terms

SUMMARY

- Over the focus period of this report, DoD has experienced an increasing convergence of policy and doctrine. This is, in part, owing to the passage of time that has allowed OSD and the Joint Staff to develop consensus on issues and solutions and to develop, coordinate, and publish top-level guidance, often based upon operational experiences and lessons learned.
- There also appears to be an increasing awareness that IA threats and vulnerabilities are more than an opportunity for increased funding; they are indeed real and merit the attention necessary to provide IA across the spectrum from peace to war.
- All IO/IA issues cannot be addressed simultaneously; however, critical issues have been prioritized and are being worked on. Processes are in place to address the harder issues in the long term.
- Where critical, common operational terminology is being developed.
- At the same time, there appears to be room in the current framework for warfighters to address and implement IO in the context of their unique warfighting domains, while still meeting joint warfighting requirements

SECTION 4

LEGAL

This section updates the Legal Environment section of the 2nd edition. Please note that this section builds upon the 2nd edition and does not cover all laws presented in the earlier edition. Instead, this presentation is a more in-depth analysis of recently passed or proposed legislation, as well as case law derived from information-assurance-related prosecutions.

CONTENTS

It has been an active year in the information assurance-related legal arena. Legislators continued to hone laws to empower law enforcement and prosecutors to respond to criminal acts against the information infrastructure. It is important to note that no laws were passed that limit intelligence activities. Case law, which in the U.S. legal system interprets the application of statutes, is evolving important issues in search and seizure; setting a value on cyber information, which has until recent years been set by physical standards, such as the cost of a disk or the cost of paper; and freedom of expression, which becomes an issue in bounding activities that can or cannot be prohibited by law. These are great strides forward, and proposed legislation indicates a desire on the part of the legislators for continued enhancement of the statutes in favor of protecting the information infrastructure, while ensuring the Constitutional rights of individuals.

4.1 DEFINITIONS AND CONTEXT FOR LEGAL DISCUSSION

Sections 3.0, 4.0, and 5.0 discuss the policy, legal, and regulatory environments, focusing on those laws, regulations, and policies that are most relevant to information infrastructure assurance.

For purposes of this document, the following definitions are employed:

- **Public law** is the body of legislation that defines organizations and their responsibilities, bound their activities, and is enforceable in court. The United States Code (U.S.C.) contains the statutes of the U.S. Government, the Federal laws, which apply to all persons on U.S. soil. Included in the U.S.C. is the *Uniform Code of Military Justice*, which, along with other Federal, state, and local laws, governs the members of the Armed Services. [97]

[97] The 'Lectric Law Library ™ Internet site, <http://www.lectlaw.com>

- **Regulations** are rules and guidelines established by administrative agencies that, if derived from statutes, may carry the force of law, such as the income tax codes. Congress created administrative agencies, such as the Internal Revenue Service, to establish and enforce regulations. Most Federal regulations are published in the Code of Federal Regulations and the basis may be an Executive Order. Regulations may apply to the general public, business entities, and the enforcing agency. States may create their own regulations.[98]
- **Policy** is a set of guidelines that generally apply to some subset of the population and may change with administrations. These are neither law nor regulation, and though violating policy does not subject a person to court action, it may subject him or her to administrative action levied by his or her agency. An example of policy are DoD regulations and OMB circulars.

Having defined the law, it also is important to look at other aspects that affect the law in practice. In the United States, case law contributes greatly to the way laws are enforced, and landmark cases bring about changes on a regular basis. In *O'Connor v Ortega*, 480 U.S. 709 (1987), for example, the U.S. Supreme Court ruled that searches of government offices by public employers are subject to Fourth Amendment search warrant requirements, with noted exceptions. The court found that government employees have a reasonable expectation of privacy in certain areas of their offices, especially in areas containing personal items, such as their desks and file cabinets. The court specified that searches for non-investigatory, work-related purposes, such as trying to find a file while an employee is on leave, are not prohibited, nor do they require warrants, as long as they are reasonable. The same standard of reasonableness was cited for administrative actions concerning work-related misconduct. [99]

This judgment also applies to telephones and computer systems, but there are exceptions allowed the operators of systems that are specified by statute. These will be discussed in Section 4.4.4 Operations Personnel/System Administrators. Also note that an alternative to seeking a warrant, is to ask for consent to search and have the employee present at the time of the search.

Another factor that is pertinent to how computer and other communications laws are enforced in practice is the ability of law enforcement to detect and investigate such cases in order to bring about a successful prosecution. Law enforcement's success hinges upon:

- The investigating officer's technical knowledge of computer systems, which either allows or prevents him or her from identifying a perpetrator and gathering evidence.
- The difficulties presented by investigations in cyberspace itself, such as ways in which the criminal conceals his trail.
- Legal aspects, such as establishing jurisdiction over the crime and what constitutes a legal search in cyberspace.

---

[98] Stephen Elias and Susan Levinkind, *Legal Research: How to Find and Understand the Law* (Berkeley, CA: Nolo Press, 1995), pp. 6/40-41.

[99] Robert Ellis Smith, "Searches and Surveillance in the Workplace, Privacy Journal" (undated): 1-2.

- Presenting a case that meets prosecution guidelines, which prioritize how the resources will be assigned to prosecutors' offices based upon the dollar value lost and seriousness of the crime to be prosecuted.

Congress is aggressively pursuing new statutes that will help smooth out legal problems, but the lack of consistent training in the law enforcement community is likely to persist for years. The proliferation of special computer crime centers, which can respond to emergencies and special cases, should ease the situation. DoD, military services, FBI, and U. S. Secret Service currently operate such units.

Before embarking upon a discussion of new statutes and proposed legislation, it is necessary to understand the meaning of the terminology employed therein and what those terms mean in the context of building a case for prosecution. Federal statutes lay out the elements of the crime and suggest a punishment. The wording of the statutes is important to note. If the word "and" appears between two elements, both elements must have occurred to be prosecutable under the statute; the word "or" indicates that only one element need occur. Another important concept is *mens rea* or culpable mental states. Words such as purposely, knowingly, recklessly, negligently, intentional, and criminal negligence are used to define the level of understanding with which the defendant must have acted in order to be charged under the statute. See Exhibit 4-1-1 below.

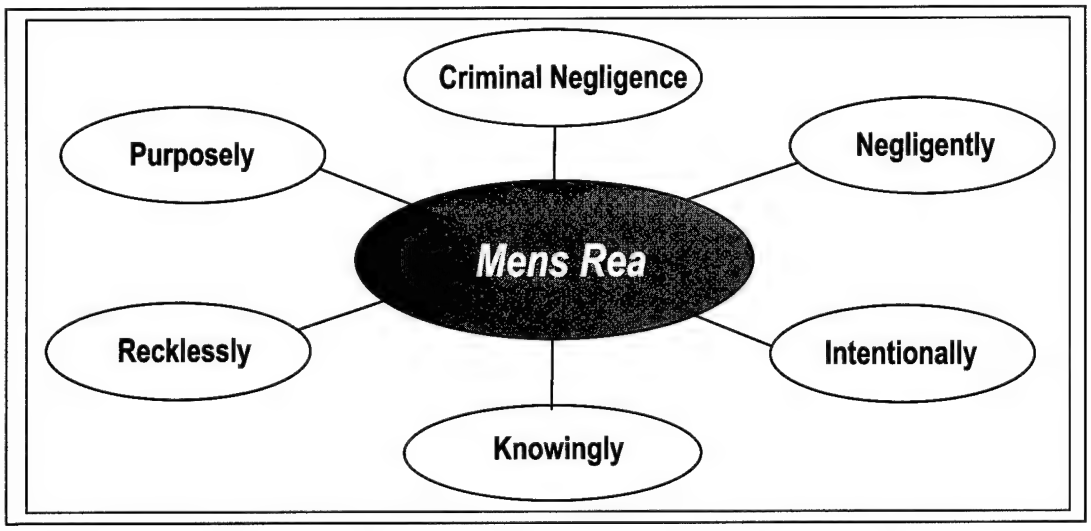


Exhibit 4-1-1. Culpable Mental States Charged under *Mens Rea*

The major statute for prosecution of DoD and active-duty military personnel for computer crime remains Title 18 U.S.C. Section 1030 (*Fraud and related activity in connection with computers*), as amended 3 October 1996, which also is known as the *Computer Fraud and Abuse Act of 1986*. Each of the elements under this statute contain words such as purposely and knowingly. The *Uniform Code of Military Justice* (UCMJ) is codified at Title 10 U.S.C. It defines crimes and describes punishments for members of the military service, but provides certain avenues not available under civilian law. Both the civilian titles and UCMJ will be discussed in this document.

The Definitions and Background section is followed by a section that discusses information assurance-related legislation, proposed since July 1996. The rest of the Legal Section contains analyses of legislative limits on infrastructure protection, UCMJ information assurance authorities, implications for the law enforcement, intelligence, system operator communities, and relevant case law.

4.2 RECENT LEGISLATION

Significant legislation passed since July 1996 includes an amendment to Title 18 U.S.C. Section 1030 (*Fraud and related activity in connection with computers*), and the *Economic Espionage Act of 1996* codified at Title 18 U.S.C. Section 1831-1839.

4.2.1 Title 18 U.S.C. Section 1030

Computer crime historically has been prosecuted under various Title 18 U.S.C. sections. Examples include: Section 1343 (fraud by wire), Section 1363 (malicious mischief), Section 1029 (access devices), Section 1030 (computer fraud and abuse), Section 785 (communicating a threat), and Section 251 (wiretap). *The National Information Infrastructure Protection Act of 1995* was an attempt to reform Title 18 of the U.S.C. and bring the necessary options for prosecuting under Section 1030. It is intended that all future finetuning of the statutes that becomes necessary as new technologies develop should be focused at Section 1030. Title 18 U.S.C. Section 1030, as amended 3 October 1996, generally prohibits gaining unauthorized access or exceeding authorized access to computers, as well as attempts to obtain such access. The acts of gaining or attempting to gain unauthorized access and exceeding authorized access to obtain information are essential elements of the crimes. National security, financial, and medical information are specifically extended protection under this section, and Section 1030 (a)(2)(C) protects against interstate or foreign theft of any information by computer. Also, of note is the fact that "obtaining information" includes the act of reading information.

The statute specifies that it does not prohibit lawfully authorized law enforcement or intelligence agency actions. The U.S. Secret Service has primary investigative jurisdiction under this statute.

Punishment ranges from 1 to 20 years and/or fines, with the heaviest punishments unauthorized or exceeded access to and disclosure of national security information, as described in (a)(1). Civil action is allowed for compensatory damages and injunctive or other equitable relief. Civil damages are limited to economic damages.

The following important definitions are found in Section 1030:

A **protected computer** is one that is:

> (A) exclusively for the use of a financial institution or the U.S. Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the U.S. Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communications.

Damage means "any impairment to the integrity or availability of data, a program, a system, or information, that

(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety.

The *Computer Fraud and Abuse Act*, as amended in October 1996, is briefed in Exhibits 4-2-1 and 4-2-2. Note the *mens rea* wording: "knowingly," "with reason to believe," "intentionally," and so forth. Also, it is worth noting that the Government must prove that a certain person or persons committed the crime, not just that a particular computer was used. This is often done through telephone record analysis and physical surveillance.

(a) Whoever - (1) Knowingly accesses a computer to obtain information that is protected "against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the *Atomic Energy Act of 1954*: "With reason to believe that the information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation" willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to do so, to any person not entitled to receive it;

(2) Intentionally accesses a computer to obtain information concerning credit or financial transactions; information from any department or agency of the United States; information from any protected computer if the conduct involved an interstate or foreign communication;

(3) Intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses a such computer affecting its use by or for the Government of the United States;

(4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, to further the intended fraud and obtains anything of value, "unless the object of the fraud and the thing obtained consist only of the use of the computer and the value of such use is not more than $5,000 in any one-year period."

(5) (A) Knowingly causes the transmission of "a program, information, code, or command," and causes damage to a protected computer;

(B) Intentionally accesses a protected computer without authorization and recklessly causes damage;

or

(C) Intentionally accesses a protected computer without authorization and causes damage;

(6) Knowingly and with intent to defraud traffics a password or similar information through which a computer can be accessed without authorization, if -

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States:

(7) With intent to extort money or a thing of value, transmits in interstate or foreign commerce any threat to cause damage to a protected computer.

And, whoever attempts to commit an offense described above.

Exhibit 4-2-1. *Computer Fraud and Abuse Act* Elements of the Crime

(c)(1)(A) "a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1), "which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(c)(1)(B) a fine and/or imprisonment for not more than twenty years for a violation of subsection (a)(1), which occurs after a conviction for another offense under this section or an attempt to commit an offense punishable under this subparagraph;

(c)(2)(A) a fine and/or imprisonment for not more than one year for committing an offense under subsection (a)(2), which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(c)(2)(B) a fine and/or imprisonment for not more than 5 years for an offense under subsection (a)(2) if - (i) the offense was committed for commercial advantage or private financial gain;

(ii) "the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) "the value of the information obtained exceeds $5,000;"

(c)(3)(A) "a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1), "which occurs after a conviction for another offense under subsection (a)(2), (a)(3), or (a)(6) of this section or an attempt to commit an offense punishable under this subparagraph;" and

(c)(3)(B) "a fine and/or imprisonment for not more than five years for a violation of subsection (a)(1), "which does not occur after a conviction for another offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section or an attempt to commit an offense punishable under this subparagraph;" and

(c)(3)(C) "a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1), "which occurs after a conviction for another offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or

(a)(7) "of this section or an attempt to commit an offense punishable under this subparagraph."

Exhibit 4-2-2. *Computer Fraud and Abuse Act* Punishments

4.2.2 Title 18 U.S.C. Section 1831 - Section 1839

The *Economic Espionage Act of 1996*, codified at Title 18 U.S.C., Chapter 90-Protection of Trade Secrets, Section 1831 - 1839, recognizes that foreign government and other agents are attempting to gain economic advantage by stealing information that is not necessarily considered national security information. The *Act*, therefore, extends Federal protection to trade secrets. While establishing new avenues for prosecution, the *Act* specifies that it does not preempt or displace other remedies. The *Act* specifies the actions of downloading, uploading, and transmitting as elements of the crime, and amends Section 102 (Wire and electronic communications interception and interception of oral communications) and Section 2516(1)(c) to include economic espionage.

> New laws became necessary because prior state and federal legislation had not kept pace with the rapidly changing technological environment. For example, if an individual downloads a computer program code onto a disk without the permission of the code owner, has a theft occurred, even though the true owner never lost possession of the original code? If a theft occurred, is the value of the material taken determined by the value of the disk on which the code is now recorded or the value of the code itself? Although Congress had enacted patent and copyright protection laws, computer crime statutes, and laws designed to prevent government employees from wrongfully disclosing proprietary information obtained by virtue of their official duties, no federal law protected, in a systematic, principled manner, trade secrets from theft and misappropriation. Legislation in the states varies but, in general, offers inadequate protection to victims of trade secret theft. [100]

The sections of the *Act* are briefed as follows. Note how the *Act* is constructed to address the intangible aspects of information, which is vital in prosecuting information-assurance-related matters and is a stride forward in promoting such legal thinking.

Section 1831 — Economic Espionage: (Agent of Foreign Power); Penalties: Persons - $500,000, 15 years; Organizations: $10,000,000. This section refers to economic espionage committed by or connected with a foreign power. Legitimate reporting activities of embassy personnel, such as gross national product data, publicly available commerce figures and agricultural output are not proscribed by the *Act*. As with other espionage statutes, the prosecutor must demonstrate the perpetrator's intent to aid the foreign power.

Section 1832 — Theft of Trade Secrets: (Commercial Espionage); Penalties: Persons: $500,000, 10 years; Organizations: $5,000,000. This section addresses the theft, misappropriation, wrongful conversion, duplication, alteration, or destruction of a trade secret. In prosecuting under this section, the prosecutor must show the perpetrator's intent to "convert a trade secret to the economic benefit of someone other than the rightful owner and intended to or knew that the

---

[100] Patrick W. Kelley, "The Economic Espionage Act of 1996," *The Law Enforcement Bulletin,* U.S. Department of Justice Federal Bureau of Investigation (1 July 1997). FBI Law Enforcement Bulletin Internet site, http://www.fbi.gov/leb/leb.htm

offense would harm or injure the rightful owner. Prosecutors also must show that the accused knowingly engaged in the misconduct charged." [101] This high threshold of proof is intended to separate criminal conduct from innocent or careless conduct.

Section 1833 — Exceptions: Law enforcement activity is exempt.

Section 1834 — Criminal Forfeiture: In addition to any other sentence imposed, the court may order the convicted perpetrator to forfeit: (1) any property derived from violation, (2) any property used to commit or facilitate commission of violation, (3) victim restitution from Victims' Fund.

Section 1835 — Orders to Preserve Confidentiality: Court may take action to preserve confidentiality of trade secrets. Such confidentiality is intended to encourage victim reporting.

Section 1836 — Civil Proceedings to Enjoin Violations: This section allows the United States Attorney to seek civil remedies to prevent and restrain violations of the *Act*. These actions include ordering persons to divest themselves of interest in an enterprise; imposing restrictions on future activities or investments of persons who may wish to engage in activities similar to the illegal activity charged; dissolving or reorganizing an organization.

Section 1837 — Applicability to Conduct Outside the United States: Extraterritorial jurisdiction applies if (1) offender is a citizen or permanent resident alien, or an organization organized under the laws of the United States; (2) an act in furtherance of offense was committed in the United States.

Section 1838 — Construction with Other Laws: The *Act* does not preempt or displace other remedies, such as state laws.

Section 1839 — Definitions: (3) (Trade Secret): A trade secret is defined as a reasonably protected property, intangible or tangible, having economic value.

4.2.3 *Telecommunications Act of 1996*

The *Telecommunications Act of 1996* is covered in detail under Section 5 of this document, the Regulatory section.

The United States' 1996 *Telecommunication Act* seeks to ensure the opportunity for free competition, fairness, and adequate enforcement within the United States' telecommunications industry. The United States has promulgated these ideals through its strong support of international agreements, such as the World Trade Organization's (WTO) 1997 *Basic Telecommunications Services Agreement* and the 1995 *Information Technology Agreement,* which reduce tariffs, establish pro-competitive regulation, and open information technology markets in over 90 percent of the WTO's 130 member nations. When the *Basic*

[101] Ibid.

Telecommunications Services Agreement is fully implemented (by 1 January 1998), U.S. corporations can establish a presence in foreign nations and acquire, in whole or in part, ownership of foreign telecommunications companies. In this way, the United States may help ensure the availability of information services by eliminating the need to use undesirable systems. The agreement also opens the door for foreign entities to operate in the United States and acquire ownership of U.S. corporations. [102]

DISA General Counsel, in its analysis of the *Telecommunication Act*, raises concerns for the Department of Defense. These concerns are also pertinent to the *Basic Telecommunications Services Agreement.* The General Counsel analysis states the following: "The language of both House and Senate versions of the *Act* when it went to conference committee contained extensive provisions dealing with foreign ownership of telecommunications companies. These provisions raised some serious national security concerns. Almost all of these provisions were eliminated in conference. Only one survived — a provision which lifted a restriction against having foreign officers and directors in certain U.S. companies. Foreign ownership issues continue to percolate in Congress and before the Federal Communications Commission (FCC) and they raise serious national security concerns." [103]

4.2.4 Electronic Freedom of Information

Implementation of the *Electronic Freedom of Information Act* (EFOIA) began 1 April 1997. The law, an update to the 1966 *Freedom of Information Act* (FOIA), was passed in September of 1996. The law requires that agencies provide electronic copies of reports, discussions, and paper, via the Internet or on CD ROMs or diskettes. Items such as E-mail can be requested under the *Act.*

When the original FOIA was passed in 1966, there was a flood of requests from persons and organizations, including foreign embassies. The result of early FOIA requests was sometimes the revelation of more information than required, such as the names and other descriptors of personnel or information that was useful in discovering confidential sources of information. This presented problems for certain law enforcement investigations and even endangered lives. It will be interesting to see what types of electronic information will be requested by persons with malicious intent toward the Government information infrastructure, such as hacker groups or foreign intelligence organizations.

While EFOIA extended the time allowed for answering requests from 10 to 20 days, the new *Act* levies extensive requirements of each agency involved. The *Act* requires that each agency maintains electronic records to promote wider access; submits an EFOIA section in its annual report to Congress; and satisfies EFOIA requirements established by the Attorney General in October 1966. In addition, each agency must track and report the following information:

---

[102] Charlene Barshefsky, Statement of Ambassador Charlene Barshefsky: "Basic Telecom Negotiation" (15 February 1997). U.S. Trade Representative Internet site, http://www.ustr.gov/agreements/telcom/barshefsy.html

[103] *Telecommunications Act of 1996.*

- Total fees collected for processing requests
- Estimated time expended processing different types of requests
- Number of full-time staff dedicated to processing FOIA requests
- Number of requests denied and reason for denials
- Number of appeals, result of appeals, and reason an appeal is denied
- Complete list of all statutes upon which the agency based decisions to withhold information
- Number of requests received and processed.

4.3 PROPOSED LEGISLATION

On 17 June 1997, F. James Sensenbrenner, Jr., (R-WI) Chairman, United States House of Representatives Committee on Science, announced the introduction of H.R. 1903, the *Computer Security Enhancement Act of 1997*. The legislation is aimed at strengthening computer security throughout the Federal government. The legislation updates guidance given in the *Computer Security Act of 1987* to accommodate the many technological advances that have occurred since 1987.[104]

In his press release, Sensenbrenner cites a General Accounting Office (GAO) finding that, owing to inadequate security in "Federal civilian computer systems," which GAO characterizes as "an enormous problem," Federal computer security is a high-risk, government-wide problem.

The *Computer Security Act of 1987* (P.L. 100-235) named the National Institute of Standards and Technology as the lead agency for computer security for Federal civilian agencies. The 1987 *Act* assigned NIST the task of developing standards and guidelines to ensure cost-effective security and privacy of sensitive information in Federal computer systems.

According to the press release, the 1997 bill's major provisions and updates are as follows:

- Requires that NIST promote the acquisition and usage of already existing computer security technology
- Increases the input of the Computer System Security and Privacy Advisory Board into NIST's decision-making process
- Develops standardized tests to evaluate the strength of foreign encryption products

[104] United States House of Representatives Committee on Science, Press Release on H.R. 1903, the Computer Security Enhancement Act of 1997, by F. James Sensenbrenner, Jr., Chairman (17 June 1997) on Internet at http://www.house.gov/science/welcome.htm, United States House of Representatives Committee on Science Internet site.

- Limits NIST's involvement to assisting Federal agencies in the acquisition of security technologies and not restricting the production or use of encryption by the private sector
- Updates the *Computer Security Act of 1987* to account for changes in technology over the last decade
- Establishes an academic fellowship program for graduate and undergraduate students studying computer security.

Congressional opponents of the administration's policy on encryption are renewing efforts to lift the export restrictions. Senators Conrad Burns (R-MT) and Patrick Leahy (D-VT) both have introduced bills that would effectively end the restrictions and outlaw mandatory key escrow, while Rep. Bob Goodlatte (R-VA) has reintroduced a bill in the House that would do the same.[105] The Administration supports a voluntary key management system for public-key-based encryption and is focusing on developing a key-management infrastructure to support those products. The following quote summarizes the aim of legislation the Administration is supporting which would:

- Expressly confirm the freedom of domestic users to choose any type or strength of encryption.
- Explicitly state that participation in the key management infrastructure is voluntary.
- Set forth legal conditions for the release of recovery information to law enforcement officials pursuant to lawful authority and provide liability protection for key recovery agents who have properly released such information.
- Criminalize the misuse of keys and the use of encryption to further a crime.
- Offer, on a voluntary basis, firms that are in the business of providing public cryptography keys the opportunity to obtain Government recognition, allowing them to market the trustworthiness implied by Government approval.[106]

4.4 LEGISLATIVE AUTHORITIES

This section addresses elements of information assurance-related crimes, as well as some options available under the *Uniform Code of Military Justice*. As case law defines how laws may be applied in practice and frequently how law enforcement may pursue a violation without impinging upon the rights of citizens, a section on pertinent case law is included.

---

[105] "Export Granted for 56-Bit Encryption," *InfoSecurity News* 8 (May 1997) 3:14.

[106] William A. Reinsch, *Administration Encryption Policy,* testimony before the Subcommittee on International Economic Policy and Trade House Committee on International Relations, 8 May 1997. United States Department of Commerce, Bureau of Export Administration Internet site, http://www.bxa.doc.gov/warcong7.htm

4.4.1 *Uniform Code of Military Justice*

As any person residing in the United States, active-duty military and DoD civilian employees can be charged with violations of Federal, state, and local statutes. The major statute for prosecution of DoD and active-duty military personnel for computer crimes remains Title 18 U. S. C. Section 1030. However, the *Uniform Code of Military Justice* (UCMJ), codified at Title 10 U.S.C. Chapter 47, gives the U.S. Government additional options for courts-martial of active-duty military personnel.

The following discussion of UCMJ Articles 92 through 134 is quoted with permission [107] from *Legal Guide to Computer Crime (A Primer for Investigators and Lawyers),* which is a comprehensive reference of statutes, case law, and procedures for investigating and prosecuting computer crime cases. Although the purpose of the document is for investigating and prosecuting cases within the DoD, the document would be highly useful to outside agencies as well. [108]

Article 92: Failure to Obey Order or Regulation. Makes it unlawful to violate or fail to obey any lawful general order or regulation. Can be used in conjunction with punitive Service regulations. Further research will be needed, at the time of the incident, to see what punitive Service regulations were in effect at the time of the alleged criminal act. The status, again at the time of incident, of the definition of a lawful general order (and whether the definition includes federal computer crime statutes) will also need to be researched. [109]

Article 106(a): Espionage. Any Service member who transmits a document or other information with the intent or reason to believe that the document or other information will be used to injure the United States (or to the advantage of a foreign nation), is subject to court martial for espionage.[110]

Article 107: False Official Statements. Using another's password could constitute a false official statement. No distinction should be made whether the entity receiving the statement was a person or a machine. The investigator and attorney should key on whether the statement or password was required for gaining illegal access to the computer system. The focus must be on "an official statement," and whether logging onto a computer is an official statement.[111]

Article 121: Larceny and Wrongful Appropriation. Defines larceny and wrongful appropriation as the wrongful taking, obtaining, or withholding, "by any means, from the possession of the owner or any other person any money, personal property, or article of value of any kind." The object of the computer theft, however, must be tangible property, such as a printed document. [112]

---

[107] Permission granted by Robert E. Giovagnoni, General Counsel, President's Commission on Critical Infrastructure Protection.
[108] Department of the Air Force, Office of the Staff Judge Advocate, Air Force Office of Special Investigations *Legal Guidance*, by Elizabeth A. Banker, Robert E. Giovagnoni, Alexander R. Smith, and John T. Soma (1996).
[109] Ibid., p. 6.
[110] Ibid., p. 6.
[111] Ibid., pp. 6-7.
[112] Ibid., p. 7.

Article 123: Forgery. The Article has been used to prosecute a subject for the altering of keypunch cards before the cards were used to process payroll checks by the computer. *United States v. Langston,* 41 C.M.R. 1013 (1970). The subject's action allowed him to increase his payroll check. Even though the accused did not actually make false writings, his actions in altering the computer input to increase the face amount of the check constituted a forgery. This analogy should hold true in all instances where a person has altered the computer's operation, at either the input or programming states, to effect the creation of a false writing.

Article 132: Frauds Against the United States. Makes punishable frauds against the United States. May provide a better remedy than forgery in those instances where the individual submits paperwork to set the computer crime in motion instead of altering the computer program. Entering false documents to receive a payroll or TDY check would be an example. [113]

Article 134: General Article. This general article has been used for theft of intangible items such as time or services. Prohibits anyone from willfully and unlawfully altering, concealing, removing, mutilating, or destroying a public record. The removal of a computer record will probably entail making a copy of the record, thereby leaving the original unaltered so as to minimize detection. Copying a computer record may be punishable under Article 134 by incorporating the same theory used in *United States v. DiGilio.* 538 F. 2d 972 (3rd Cir. 1976). In *DiGilio*, the defendant made unauthorized photocopies of FBI files using Government equipment. The unauthorized copies were considered Government records and the removal of the copies constituted theft under section 641. The court held that "any record" under 641 also included the content of the record. [114]

Case Law Involving UCMJ

U.S. v James A. Maxwell [45 M.J. 406 (1996)], decided 21 November 1996, demonstrates several of the issues involved in prosecuting cyber cases. It also demonstrates how a case can be begun by a civilian agency, then prosecuted under the UCMJ.

Colonel James A. Maxwell, U.S. Air Force, was convicted by general court-martial under Article 134 UCMJ of two specifications of using his personal computer to transport obscenity and child pornography. On 21 November 1996, the U.S. Court of Appeals for the Armed Forces affirmed his conviction, but decided in his favor on certain issues, notably certain of his claims that his Fourth Amendment rights were violated in the original and subsequent searches.

The facts of the case are quoted from court records as follows:

> In December 1991, Roger D. Dietz, a resident of California and subscriber to America On Line (AOL), reported to the press that child pornography was being distributed on AOL. He made this report after contacting his local police department and receiving little assistance. The press contacted AOL representatives who then called the FBI, who then contacted Mr. Dietz. He had

[113] Ibid., p. 7.
[114] Ibid., p. 7.

> also by this point forwarded several E-mail messages to AOL's vice-president of marketing, Ms. Jean Villanueva. Mr. Dietz provided copies of E-mail messages that he had received, along with graphics files (GIFs) to Ms. Villanueva, who gave them to FBI Agent Garrett. Agent Garrett opened an investigation and contacted AOL in order to obtain more information about the identities of the individuals using the screen names who appeared to be transmitting child pornography. When Agent Garrett contacted AOL for this purpose, he was informed that he would need a warrant in order to receive this information. [115]

The search warrant Agent Garrett obtained included approximately 80 screen names, which included a user list, as well as some of the child pornography that Dietz received from individuals on the user list.

> Not all the GIFs were obviously obscene or involved minors. Further, on cross-examination, the AOL expert, Mark Seriff, stated that it would be impossible from just viewing the warrant, its attachments, and the affidavit to determine which user sent which graphic image. He stated that the agent would need at least one other list — an 'E-mail chain' — to be able to determine who sent the pictures attached to the warrant. [116]

Unbeknownst to Agent Garrett, AOL wrote a software program to search its own system, based upon information received from Dietz. The result of the search conducted by AOL via this program was 12,000 to 14,000 pages of computer fan-folded sheets and 39 high-density disks. At issue in court was: exactly when did AOL run this program — Agent Garrett testified that he handed AOL the warrant and they handed him the pre-run documents, while AOL testified that they did not search their system until the warrant had been received — and whether the resultant search was more expansive than the federal search warrant. Also, an error was made in transcribing one of Maxwell's screen names from "REDDE1" (ready 1) to "REDDEL." AOL's search utilized the correct name. A third point was that the AOL search produced transmissions under the screen name "Zirloc."

After reviewing the information obtained through the search warrant, the FBI discovered that the subject of the investigation was an Air Force member and contacted the AFOSI. The FBI turned over a copy of all seized material and AFOSI opened its own investigation on Col. Maxwell.

It was determined that many of the Zirloc transmissions were to a junior Air Force officer known as "Launch Boy." [117] These were largely an exchange of sexual discussions. On the basis of this information, AFOSI sought and received a search authorization for Maxwell's quarters to seek evidence related to Maxwell or whether Maxwell had possessed and/or transmitted obscene materials. Pursuant to the warrant, AFOSI seized Maxwell's Apple Macintosh computer, which

---

[115] 45 M.J. 406 (1996), p. 412.
[116] Ibid., p. 413.
[117] Ibid., p. 414.

they searched and from which they downloaded three visual depictions that were admitted into evidence as child pornography. [118]

In his appeal, Maxwell argued, among other things, that the original warrant was overly broad and thus violated his Fourth Amendment rights, and also that the warrant had not provided for seizure of the Zirloc materials. He further argued that the Zirloc materials were not subject to the "good faith" rule, which allows latitude for an officer acting in good faith, and should be excluded from evidence. He challenged the military search authorization by claiming that the magistrate had used personal standards rather than legal standards in determining probable cause. [119] In addition, he said that the military magistrate had relied upon "fruits of the poisonous tree" from the FBI warrant in making his decision. Maxwell also questioned the jury instructions on the basis that the judge did not instruct the jury that they must know the children depicted were minors and improperly gave the "community standards." Maxwell argued that the language in question in his case, whether indecent or not, was protected by the First Amendment. Finally, Maxwell argued that the sentence to dismiss him from military duty constituted cruel and unusual punishment under the Eighth Amendment. [120]

The U.S. Court of Appeals for the Armed Forces findings are as follows:

- Maxwell had a reasonable, but limited, expectation of privacy in E-mail messages that he sent and/or received on a computer subscription service; but "implicit promises or contractual guarantees of privacy by commercial entities [i.e., AOL] do not guaranty constitutional expectation of privacy for purpose of deterring validity of search." [121] To this point, the court also commented, "Fourth Amendment requires that police agencies establish probable cause to enter into personal and private computer, but when individual sends or mails letters, messages, or other information on computer, individual's expectation of privacy diminishes incrementally, and the more open the method of transmission, the less privacy one can reasonably expect, for purpose of determining validity of search." [122]
- The scrivener's error in drafting search warrant for service's computers, mistakenly representing the accused's screen name with unused spelling, did not invalidate the warrant; the reason was that the FBI and AOL were both "clear as to true screen name for which they were searching." [123]
- The search warrant was not overly broad, though AOL's execution of the warrant was.
- Evidence seized under the screen name "Zirloc," which was not included in the warrant, was unlawfully seized and not admissible. The court held that the "Contents of mailbox in computer subscription service's computer belonging to screen-name

[118] Ibid., p. 414.
[119] Ibid., p. 415.
[120] Ibid., p. 416.
[121] Ibid., p. 406.
[122] Ibid., pp. 406-407.
[123] Ibid., p. 407.

identity not listed on search warrant were not admissible under 'good faith' exception, as service, which performed search, did not rely on language of warrant, but retrieved information pursuant to search program which the service developed in anticipation of warrant." Also, "Good-faith exception did not apply to seizure of contents of mailbox in computer subscription service's computer belonging to screen-name identity not listed on search warrant, given that that subscription account could be shared by family using different screen names, but billed in name of one individual; court was unpersuaded on record to declare others' expectations of privacy to be forfeited based upon undefined 'good-faith' exception." The court held that files discovered pursuant to the search conducted under Zirloc would not have inevitably been discovered in the course of a legal search and that E-mail conversations were fruits of the unlawful search, making them inadmissible as fruits of the poisonous tree. Finally, the court held that AOL's search was not a private search, as the information was gathered at the Government's request. [124]

- The military magistrate had probable cause to issue search authorization for accused's personal computer and his home for obscenity and child pornography, based upon admissible information obtained in the AOL search.
- The Government was only required to prove that accused believed subjects were minors to support child pornography conviction.
- The alleged erroneous jury instruction that the relevant community was the nationwide community as a whole afforded a more favorable standard to the accused. [125]

In the introduction to his opinion, Chief Judge Cox wrote: "This case takes us into the new and developing area of the law addressing the virtual reality of 'cyberspace,' which is the generic term for the loosely-connected network of computers that permits users of personal computers worldwide to communicate with each other. In this case, we deal with one specific computer subscription service — AOL. This service provides many self-contained communication services, such as informational bulletin boards and electronic mail (E-mail), as well as an efficient path to access the Internet. AOL is a private company that charges monthly fees based upon the type and amount of usage of their services. This case is solely concerned with AOL's E-mail service, although arguably the questions in this case may eventually arise in connection with any number of existing and constantly developing computer services. AOL E-mail allows users to communicate with other AOL subscribers on its own internal E-mail network. It is also possible to access other computer user outside the AOL subscription service, but this requires knowledge of a more lengthy and specific address of that user. [126]

"New technologies create interesting challenges to long-established legal concepts. Thus, just as when the telephone gained nationwide use and acceptance, when automobiles became the established mode of transportation, and when cellular telephones came into widespread use, now personal computers, hooked up to large networks, are so widely used that the scope of Fourth

[124] Ibid., p. 408.
[125] Ibid., p. 409.
[126] Ibid., p. 410.

Amendment core concepts of 'privacy' as applied to them must be reexamined. Consequently, this opinion and the ones surely to follow will affect each one of us who has logged onto the 'information superhighway'". [127]

Because two of the findings were reversed, Maxwell may receive another hearing.

4.4.2 Law Enforcement Implications

In its legislative analysis of the *National Information Infrastructure Act of 1996*, the Computer Crime and Intellectual Property Section of the United States Department of Justice stated the following:

> . . . computer crime creates unique problems for law enforcement and a concomitant threat to the public welfare. The most significant legislative problems stem from technology's shift from a corporeal to an intangible environment. This departure from a physical world (where items are stored in a tangible form that can be carried, such as information written on paper) to an intangible, electronic environment means that computer crimes (and the methods used to investigate them) are no longer subject to traditional rules and criminal mischief have evolved. Before the advent of computer networks, the ability to steal information or damage property was to some extent determined by physical limitations. A burglar could break only so many windows and burglarize only so man homes in a week. During each intrusion, the burglar could carry away only so many items. This does not, of course, make this conduct trivial, but it points out that the amount of property a burglar could steal, or the amount of damage he could cause, had physical limits. [128]

The analysis states that these limits do not apply to crimes involving the use of information systems because the criminal is no longer limited by his or her ability to travel. "The quantity of information stolen or the amount of damage caused by malicious programming code may be limited only by the speed of the network and the criminal's computer equipment." [129]

The case of Julio Cesar Ardita, a 21-year-old from Buenos Aires, Argentina, is a case in point. On 29 March 1996, Attorney General Reno announced that Federal agents had used a court-ordered wiretap on a computer network, and had identified Ardita as a hacker who was breaking into sensitive U.S. military and space computer systems. Authorities had developed minimization techniques as the wiretap was intercepting hundreds of thousands of innocent messages through a network operated by Harvard University. Investigators had identified key programs, words, and phrases that were unique enough to be reasonably linked to Ardita's pattern of activities. Having determined this profile and developed enough probable cause to get the court to order a wiretap, investigators programmed a computer to analyze traffic through the

---

[127] Ibid., p. 410.
[128] Department of Justice, Computer Crime and Intellectual Property Section, *Legislative Analysis: The National Information Infrastructure Protection Act of 1996* (undated).
[129] Ibid.

network and indicate those that matched Ardita's pattern. In that manner, the investigators minimized intrusion into the activities of persons who were probably innocent. The result of employing these minimization procedures was that only two of the flagged messages were determined not to be Ardita's. Investigators analyzed telephone records to confirm that Ardita's phone was actually being used to access the Harvard network.

Ardita, who ran "Scream," a bulletin board for hackers, was charged with using stolen accounts and passwords to gain access via the Internet to computers at the Naval Command Control and Ocean Surveillance Center, the Naval Research Laboratory, the Jet Propulsion Laboratory, Ames Research Center, and the Los Alamos National Laboratory. The files he accessed were not classified, but were considered sensitive government information concerning satellite engineering, radiation, aircraft design, and radar technology.

The result of approximately 9 months' work that involved multiple investigators and Government attorneys is that a warrant was issued for Ardita's arrest. The catch is that the extradition treaty between the United States and Argentina does not provide for extradition under these circumstances. Instead, Argentinean authorities seized his computer equipment.

Communications Assistance for Law Enforcement Act of 1994

The *Communications Assistance for Law Enforcement Act of 1994* (CALEA) was designed to ensure that telephone companies can accommodate all Federal, state, and local law enforcement agency court-approved intercept needs through 1998 and beyond. It was intended to protect this capability despite changing technologies that could inhibit electronic surveillance. CALEA does not give law enforcement any new authority in obtaining or conducting electronic surveillance and should not, in and of itself, result in an increase in the use of the technique. Section 104 of CALEA requires that the Attorney General publish in the Federal Register and give notice to telecommunications carriers of: 1. the actual number of simultaneous communication interceptions, pen registers, and trap-and-trace devices that the Attorney General estimates will be needed by October 1998 ("actual capacity"); and 2. the maximum capacity that will be required to accommodate all simultaneous communication interceptions, pen registers, and trap-and-trace devices that the Attorney General estimates will be needed after October 1998 ("maximum capacity"). [130]

According to the FBI, approximately 90 percent of the estimated capacity will be used for pen registers and trap-and-trace devices. "In addition to the Federal government, 41 states, Puerto Rico, the Virgin Islands, and the District of Columbia have statutes allowing for the use of court-authorized wiretaps by law enforcement in the investigation of the most serious criminal acts. All states provide for law enforcement access to dialed telephone numbers using the less intrusive pen registers and trap and trace devices . . ." [131]

---

[130] Department of Justice, Federal Bureau of Investigation "Implementation of Section 104 of the Communications Assistance for Law Enforcement Act: Second Notice and request for comments," *Federal Register* 62 (14 January 1997) 9.
[131] Ibid.

The FBI has stated that law enforcement has thus far enjoyed the ability to carry out virtually all court-ordered electronic surveillance successfully. New technologies, such as modernized telephone systems, may limit this ability. CALEA does not suggest technological solutions for effecting electronic surveillance; it only seeks to ensure that the required capacity of telephone equipment, facilities, and services is available to law enforcement.

The FBI published in the *Federal Register* an Initial Notice for Comment on 16 October 1995. Owing to extensions, the Second Notice for Comment was published on 14 January 1997. The period for comment on the Second Notice closed 5 June 1997. The Final Notice is yet to be published.

Difficulties Inherent in Prosecuting Crimes Involving Information Systems

- **The Nexus of Intent.** The Supreme Court decision in *Brandenburg v. Ohio* [395 U.S. 444 (1969)] states that speech may not be punished unless it is "an incitement to imminent lawless action." In criminal prosecutions, it is necessary to show a nexus between the action and the result. A commonly-cited example is the man who stands up in a theater and shouts "fire," causing several people to be trampled as the crowd attempts to flee. There is a clear nexus between his words and the action that caused several people to be injured. Freedom of speech over the Internet interjects a difficulty in proving a clear nexus between words and subsequent actions. At issue here is whether information such as how to make bombs is merely informative or is designed to incite others to illegal action. Noting that such information has been distributed in print for decades, it is difficult to make the case that the appearance on the Internet is somehow more likely to incite illegal action.

- **Jurisdiction.** Recent case law supports the idea that a state may exercise personal jurisdiction over a resident of another state on the basis of the fact that the person maintains a web site that is accessible in all states, which enables him or her to defraud a resident of the state that seeks jurisdiction. The tests applied in the past are derived from *International Shoe Co. v. Washington*, 362 U.S. 310 (1945), which said that in order to establish jurisdiction over a non-resident defendant, the non-resident defendant must have either (1) "substantial, continuous and systematic" presence in the forum state, which would give the court general jurisdiction over the defendant, or (2) certain "minimum contacts" with the forum state such that maintenance of the suit does not offend "traditional notions of fair play and substantial justice." When the court is deciding whether the defendant has a continuous and systematic presence in a state, it looks at the number of "hits" or customers that a web site has received from the state and evaluates the "totality of circumstances: to evaluate the relationship among the defendant, the forum, and the litigation." (A "hit" is a download of a web page.) *Calder v. Jones*, 465 U.S. 783 (1984). The court did not establish a particular number of "hits" to define jurisdiction.[132]

---

[132] Dennis F. Hernandez and David May, "Personal Jurisdiction and the Net: Does Your Website Subject You to the Laws of Every State in the Union?", *Los Angeles Daily Journal* (July 15, 1996) reprinted by the UCLA Online Institute for Cyberspace Law and Policy, http://www.gse.ucla.edu/iclp/dhdm.html

Courts also have said that a state can assert jurisdiction based upon "minimum contacts." To fit the requisite "minimum contacts," the nonresident defendant must (1) "purposefully direct his activities or consummate some transaction with the forum or its residents," (2) the claim must arise out of or relate to the defendant's forum-related activities, and (3) the exercise of jurisdiction must be fair and just. See *Core-Vent v. Nobel Industries* AB, 11 F. 3d 1482, 1485, (9th Cir. 1993). In *California Software, Inc. v. Reliability Research*, 631 F. Supp. 1356, 1361 (C.D. Cal. 1986), the court said, in relation to a statement posted on a bulletin board service, that "[t]he mere act of transmitting information through the use of interstate communication facilities is not . . . sufficient to establish jurisdiction." [133]

This rather ambiguous trend continues in the following, which are recent cases concerning personal jurisdiction in cyberspace:

- In *CompuServe v. Patterson*, 89 F.3d 1257 (6th Cir. 1996). "The Sixth Circuit held that keystrokes at a computer terminal can generate contacts with a party in another state substantial enough to justify the exercise of personal jurisdiction in that state." [134]

- *Maritz, Inc. v. Cybergold, Inc.*, Case No. 96V01340 (August 19, 1996). "Maritz, a Missouri plaintiff, had sued Cybergold under the *Lanham Act*. Although defendant's only contact with the state of Missouri was through its web site (which was presumably maintained in Berkeley, California), the U.S. District Court for the Eastern District of Missouri ruled that it had personal jurisdiction over Cybergold." [135]

- *State v. Granite Gate Resorts, Inc.* (pending). In this case, the Minnesota Attorney General has brought a civil action against the owners of a Nevada web site advertising an online gambling service. Defendant has filed a motion to dismiss for lack of personal jurisdiction, and the attorney general has filed a memorandum of law in opposition." [136]

There were, however, decisions to the contrary:

- *Bensusan Restaurant v. King*, 1996 U. S. Dist. Lexis 13035 (9 September 1996) "The U.S. District Court of the Southern District of New York held that the court did not have personal jurisdiction over the nonresident defendant, whose only contact with New York was its web site, which was presumably located in Missouri." [137]

---

[133] Ibid.

[134] The University of California Los Angeles (UCLA) Online Institute for Cyberspace Law and Policy, *Personal Jurisdiction: An Emerging Controversy Heats Up,* 1 October 1996. On UCLA's Internet site at http://www. gse.ucla.edu/iclp/cyberjurisd.html

[135] Ibid.

[136] Ibid.

[137] Ibid.

- *McDonough v. Fallon McElligott* (1996) "The U.S. District Court for the Southern District of California dismissed a copyright infringement action for lack of personal jurisdiction over the defendant, whose principal contact with California was the accessibility of its web site to California residents." [138]

Also, in *Network Solutions, Inc. v. Clue Computing, Inc.*, 1996 U.S. Dist. Lexis 18013 (D. Col. 1996), the court found no subject matter jurisdiction in a domain name lawsuit under the Federal interpleader statute. [139]

- **Extradition.** As discussed in detail in Section 8, International Aspects of Information Assurance, extradition can be a major problem for law enforcement in prosecuting cases where the defendant is located outside the United States. What is an offense in the country requesting extradition may not be against the law in the country receiving the request. Typically in such situations, the receiving country will not extradite. If the action in question is a crime in the United States and is committed via the Internet from another country, the country where the defendant resides may also wish to prosecute and so may not be willing to extradite. As mentioned above, Julio Cesar Ardita has been charged with breaking into U.S. Government computers, among other offenses. Ardita resides in Argentina and the computer crimes alleged are not an extraditable offense under the U.S. treaty with Argentina. [140]

- **Electronic Discovery.** During the pre-trial process, each side uses the discovery process to attempt to learn what the other side will argue about the case. There are specific procedures allowable for discovery: depositions, interrogatories, admissions of facts, production of documents. In deposition, the parties are questioned by attorneys under oath and their statements are recorded by a court reporter. Interrogatories are written questions, which may be used to ask parties to identify the source and validity of documents that may be introduced as evidence at trial. Admissions of facts are determined when one party sets out a list of facts to the other, and the receiving party either admits or denies these facts. Anything not denied is considered admitted. Production of documents is when one party asks another to produce specific documents. [141]

  In fact, the scope of information obtainable through discovery is quite broad and not limited to what can be used in a trial. Federal courts and most state courts allow a party to discover any information "reasonably calculated to lead to the discovery of admissible evidence." Because of this broad standard, parties often disagree about what information must be

---

[138] Ibid.

[139] Stuart Biegel, "Reflecting Back On 1996: The Year That Cyberspace Law Came Of Age," *L.A. Daily Journal* (23 January 1997), reprinted by the UCLA Online Institute for Cyberspace Law and Policy, http://www.gse.ucla.edu/iclp/jan97.html

[140] "U.S. uses first court-ordered wiretap on computer network," *Nando.net* (29 March 1996). On Nando.net Internet site at http://www2.nando.net/newsroom/ntn/biz/032996/biz9_7625.html

[141] Elias and Levinkind, p. 3/7.

> exchanged and what may be kept confidential. These disputes are resolved through court rulings on discovery motions. [142]

The advent of electronic storage of data has exacerbated this situation. Once, attorneys had to go through stacks of paper received through the discovery process. In addition, the attorney would have to provide storage for all documents. This set some limits on the amount an attorney might request, but since an attorney can now request thousands of files on disk, it isn't as large a problem. Disks do not take up much room and there are many ways to search a disk quickly.

The Federal Rules of Civil Procedure were amended in 1970 to pertain to electronically-stored information. Rule 34 is excerpted as follows:

> Any party may . . . request . . . to inspect and copy, any designated documents (including . . . other data compilations from which information can be obtained, translated, if necessary by the [responding party] through detection devices into reasonably usable form). [143]

Everything about an electronically-stored file can be discovered, including: (1) the actual name of the file, (2) any personal notes that might not appear in the final version of a memorandum, and (3) lost or "erased" data.

4.4.3 Intelligence Community Implications

One information assurance-related issue that is specific to the intelligence community is under what circumstances it is legal to employ information warfare (IW) tactics. Per Department of Defense, Commander in Chief U.S. Atlantic Command, memorandum entitled, *Legal Aspects of Peacetime Information Warfare Command and Control*, [144] "1. Nothing prohibits the Department of Defense from using overt means to collect intelligence, or otherwise engaging in those activities necessary to support traditional military intelligence or counterintelligence missions." Covert actions by the military, however are viewed very differently. A few authoritative documents, discussed in more detail below, address this issue. What limited guidance they provide indicates that in time of peace, the military is primarily intended to fulfill a role in support of the CIA, and to a much more limited degree, the FBI. This relationship is altered dramatically, however, giving DoD a more active role when one of two events occur:

a. The nation is engaged in a war, or a period of crisis requiring a Presidential report to Congress pursuant to the War Powers Resolution;

---

[142] The 'Lectric Law Library™ Internet site at http://www.lectlaw.com/def/d058

[143] James H. S. Pooley and David M. Shaw, *The Emerging Law of Computer Networks, Finding Out What's There: Technical and Legal Aspects of Discovery* (1997). Fish and Richardson Internet site, http://www.fr.com/working publis

[144] DoD, Commander in Chief U.S. Atlantic Command, Memorandum for: IW Wargame Participants: "Legal Aspects of Peacetime Information Warfare Command and Control" (29 January 1996).

b. A Presidential finding is made authorizing DoD to take covert actions intended to achieve a particular objective.

The statutory framework for covert IW is found in Title 50, Section 4133b of the U.S. Code. This provision requires that, prior to authorizing any U.S. Government entity to engage in covert action, the President must submit a written finding to Congress which details why: a. The action is necessary to support identifiable foreign policy objectives of the United States, and b. The action is important to the national security of the United States. [145]

'Covert Action' is defined as an activity of the U.S. Government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly. Covert action intended to influence U.S. domestic political process, public opinion, policies, or media is flatly prohibited. [146]

Executive Order 12333, entitled United States Intelligence Activities, expands the statutory language. This document is binding on all elements of the Executive Branch and identifies the following division of intelligence responsibilities:

a. CIA. Designated as the only U.S. agency authorized to conduct 'special activities' (read covert actions) except when one of the two events discussed in paragraphs 1a and 1b, above, occur.

b. DoD. Responds to taskings by the Director of Central Intelligence. Also required to collect, produce, and disseminate military and military-related foreign intelligence and counterintelligence (traditional missions). Specified lead agency only in conducting signal intelligence through the National Security Agency.

c. Dept. of Treasury. Conducts overt collection of financial/monetary/foreign economic information.

d. DoS. Conducts overt collection of information relevant to U.S. foreign policy.

EO 12333 also prohibits all executive agencies from engaging in undisclosed participation in organizations within the U.S. unless agency and Attorney General approval is obtained. In any event, participation can be undertaken only on behalf of the FBI as part of a lawful investigation, or when the organization is composed primarily of individuals not U.S. persons and it is reasonably believed to be acting on behalf of a foreign power. [147]

---

[145] Ibid.
[146] Ibid.
[147] Ibid.

Decisionmakers must address certain legal factors before initiating IW plans: 1) whether to apply the law of peace or the law of war; 2) the legitimacy of the target under international law and the law of armed conflict; and 3) procedural requirements for obtaining appropriate approval for individual targets or plans. [148]

The Law of War

In an armed conflict, usually signaled by a Presidential report to Congress under the *War Powers Act*, the law of armed conflict (LOAC) applies. With most military targeting decisions offensive IW is lawful, as long as the amount of force applied is proportionate and the military commander applies the LOAC balancing test. [149]

International Law

Chapter VII of the U.N. Charter states that the U.N. Security Council may authorize its member states to use "all necessary means" to "restore international peace and security." Article 41 authorizes "measures not involving the use of armed force," such as "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication, and the severance of diplomatic relations." Article 51 justifies a nation's right to defend itself, while Article 2 (4) prohibits aggression against other states. [150]

It is important to remember that actions that are less than force may still violate international law. The "Declaration on Inadmissibility of Intervention into the Domestic Affairs of States," U.N. General Assembly Resolution 2131 (1965) states the following:

> i. No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements are condemned.
>
> v. Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State. [151]

Offensive IW in peace time could be construed to fall into the category of actions described in subparagraphs i. and v., above; while countermeasures are authorized, as long as they are of a proportionate response.

---

[148] Ibid.
[149] Ibid., p.1.
[150] Ibid., p. 2.
[151] Ibid., p. 2.

In addition, other international treaties that constrain IW. Examples of these are:

> i. U.N. Convention on the Law of the Sea - provisions on innocent passage and 'unauthorized broadcasting from the high seas.'
>
> ii. International Telecommunications Convention of 1982 (Nairobi Convention) - notification requirements to suspend international telecommunications service, and avoid 'harmful interference.'
>
> iii. Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) - requirement to provide access on a non-discriminatory basis.
>
> iv. Convention on the International Maritime Satellite Organization (INMARSAT) - use for "peaceful purposes."
>
> v. Convention on International Civil Aviation (Chicago Convention) - every state must refrain from use of weapons against civil aircraft in flight, or endangering safety of flight. [152]
>
> Every violation of international law attributed to a nation authorizes a remedy, whether in the form of countermeasures by a nation whose rights were violated, by the payment of reparation, or by the political costs in the court of world opinion. It is at this point almost entirely speculative how electronic intrusions will be treated under international law. Sovereignty is still a powerful international concept, however, and even intrusions that cause no damage will be analyzed in many cases as technical violations. [153]

4.4.4 Implications for Operations Personnel/System Administrators

The *Electronic Communications Privacy Act of 1986* (ECPA), Title 18, U.S.C. Section 2510 - Section 2711 protects data in transit, as well as stored data. The *Act* distinguishes between acquiring contents and disclosing contents. It specifies exceptions when there is a court order, consent, or to protect rights or property. This allows monitoring for law enforcement purposes, as well as an employer's right to monitor an employer-owned system. Title 18 U.S.C. Section 2511(2)(a)(i) states:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee or agent or a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property

[152] Ibid., p. 4.
[153] Ibid., p. 4.

> of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

The preponderance of case law supports the employer's right to monitor employer-owned systems. However, courts also have held that the employee has some expectation of privacy. One important, though not essential, factor in litigation is whether the employer has a written E-mail policy. If a policy states that the E-mail system is the employer's property and is to be used for business purposes only, and that messages are the property of the employer, it leaves little doubt as to reasonable expectation of privacy. Warning banners reinforce this message to the employee.

There has been considerable case law establishing the line between an employee's right to privacy and an employer's right to monitor the activities of employees E-mail. First of all, E-mail remains on the employer's server even when it has been deleted from the employee's hard drive. The court in *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E. D. Pa. 1996), held that there can be no reasonable expectation of privacy in E-mail at work that relates to the employer's business. In *Smyth v. Pillsbury*, the court stated that, despite the fact that the employer had said there was no monitoring of employee E-mail, Pillsbury's "interest in preventing inappropriate and unprofessional comments outweighed any privacy right the employee had." Smyth's comments concerning the sales management staff were that he was going to "kill the backstabbing bastards" and he referred to the holiday party as the "Jim Jones Koolaid affair." [154]

In *Bourke v. Nissan Motor Corp.*, No. B068705 (Cal. Ct. App. July 26, 1993), the California Court of Appeals affirmed an employer's right to access employees' E-mail. The plaintiffs, Bonita Bourke and Rhonda Hall, had sent messages that were personal and sexual in nature over the Nissan E-mail system. This was revealed by Bourke to another co-worker as she happened to select one of these messages as she was demonstrating the use of the system. Nissan reviewed E-mail sent by the plaintiffs and others after the incident was reported to management. Bourke resigned and Hall was terminated. "The plaintiffs sued Nissan for invasion of privacy, violation of their constitutional right to privacy, violation of the criminal wiretapping and eavesdropping statutes, and wrongful discharge in violation of public policy." [155]

The appellate court affirmed the trial court's grant of summary judgment in favor of Nissan. The appellate court said that the plaintiffs did not have a reasonable expectation of privacy because they had signed waiver forms that stated company policy that E-mail was for business purposes only. The court did not find the fact that the plaintiffs were issued passwords enough to uphold the plaintiffs' expectation of privacy. The court also rejected the claim that Nissan violated the California wiretapping statute, as accessing the E-mail did not entail use of the telephone system

---

[154] Mark S. Dicther and, Michael S. Burkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age," presented at The American Employment Law Council, Fourth Annual Conference, Asheville, North Carolina, 2-5 October 1996; and Lisa Marilyn Hill, "Electronic Mail in the Workplace," *MTTLR News* (April 1997). On University of Michigan Internet site at http://www.law.umich.edu/mttlr/news/index.html#stories

[155] Ibid.

and Nissan did not capture the transmissions in transit. The court affirmed Nissan's right as the system operator to access the system. [156]

4.4.5 Recent Case Law Addressing Constitutional Issues

As shown in *U.S. v. Maxwell*, constitutional issues are germane to cybercrime prosecutions, and court holdings concerning such issues apply to similar situations in other prosecutions. Therefore, a First or Fourth Amendment opinion on a pornography case may be used to affect a ruling in a cybertheft case. The following cases were chosen with that issue in mind.

Freedom of Expression, as well as Jurisdiction: Pornography

In *United States v. Thomas*, a freedom of expression case, the Sixth Circuit Court upheld the conviction of Robert and Carleen Thomas for violating Federal obscenity laws. The Thomases were convicted in Tennessee for selling materials deemed to be pornographic in the Memphis community. The Thomases did this from a bulletin board service they operated in Northern California. The U.S. Supreme Court refused to hear the case. [*United States v Thomas*, 74 F.3d 701 (6th. Cir. 1996); cert. denied, 117 S. Ct. 74.] [157]

Freedom of Expression: Encryption

In his testimony before the Senate Judiciary Committee hearings on encryption, FBI Director Louis J. Freeh stated: "Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes." [158] Given its potential use in international crime, it is important to consider how case law is evolving on encryption issues. As of November 1996, non-military encryption has been regulated by Export Administration Regulation (EAR), 15 CFR Parts 730-774, which makes it illegal to export encryption software that exceeds 56-bit encoding. The debate as to what constitutes freedom of expression as it pertains to encryption is still pertinent to information assurance. (See Regulatory section for a fuller discussion of the regulation of encryption.)

In cases since July 1996, the argument was put forth that the right to export encryption is protected under freedom of expression, based upon the premise that political speech is inhibited when one believes the speech can be intercepted by a government. Phil Zimmerman was convicted of violating International Traffic in Arms regulations [5. 22 U.S.C. 2778 et. seq., 22

---

[156] Ibid.

[157] Stuart Biegel, "Reflecting Back".

[158] Department of Justice, FBI, Statement before the Senate Judiciary Committee Hearing on Encryption, Washington, D.C., by Louis J. Freeh (9 July 1997).

CFR 121 et seq.] when he distributed the Pretty Good Privacy (PGP) E-mail encryption program over the Internet and the court refused to consider his freedom of speech argument. [159]

In *Daniel J. Bernstein v. United States Department of State*, [160] Bernstein also sought the right to export encryption-related technologies and information across national boundaries. Bernstein developed a private key encryption algorithm called the "Snuffle," about which he wished to publish, teach, and lecture. He sued the U.S. Department of State, alleging that sections of the *Arms Export Control Act* (AECA), and the *International Traffic in Arms Regulations* (ITAR), which restrict the export of certain encryption, are unconstitutional. Among other things Bernstein argued "that the licensing requirements under the AECA and ITAR are a content-based restriction on free speech, constitute an impermissible prior restraint on his ability to communicate and publish his source code and accompanying technical data, and are vague and overbroad." [161]

In this case, the court considered whether the use of encryption constituted speech or conduct. The court held that "[s]oftware related to encryption is simply a topic of speech employed by some scientists involved in applied research. Hence, Snuffle's speech afforded the full protection of the First Amendment not because it enables encryption, but because it is itself speech." [162] The court further held that the AECA imposes an unconstitutional prior restraint on free speech, as is the ITAR licensing system, as applied to scientific research and speech concerning encryption.

The State Department "prevailed in the related lawsuit of Karn v. Department of State, 925 F. Supp. 1 (D. D.C. 1996) (executive branch determination under *Arms Export Control Act* that a disk containing cryptographic algorithms is subject to strict export control and is not judicially reviewable).

To recap the Government's objection to allowing the use of powerful encryption: the Government believes that encryption inhibits the Government's ability to enforce court orders that are valid under the Fourth Amendment (the wiretap statute 18 U.S.C. Section 2511; and the *Foreign Intelligence Surveillance Act*, 50 U.S. C. Section 1801 *et. seq.*) The reason being that encryption converts readable text to unreadable cypher text. Per Executive Order 12924, 15 November 1996, encryption products are "designated defense articles in Category XIII of the United States Munitions List and regulated by the United States Department of State pursuant to the *Arms Export Control Act* 22 U.S. C. 2778 *et. seq.*"

---

[159] Lance Rose, *First Amendment Protection for Networks and On-Line Systems, The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues* (Computer Law Association: 1996). On Computer Law Association Internet site at http//:cla.org/RuhBook/chp10htm

[160] Daniel J. Bernstein v U.S. Department of State et al. can be found on Internet at http://www.eff.org/pub/Leagal/Cases/Bernstein_v_DoS/Legal/961206.decision

[161] Brown Raysman Millstein Felder & Steiner LLP, "California Federal Court Again Holds Encryption Software Protected by First Amendment," on Brown Raysman Millstein Felder & Steiner LLP site on Internet at http://www.brownraysman.com/docket/berstn.htm

[162] Ibid.

Meanwhile, the Commerce Department granted Digital Equipment Corp. (Maynard, Mass.), Cylink Corp. (Sunnyvale, Calif.), and Trusted Information Systems Inc. (Glenwood, Md.) the right to export 56-bit encryption software, with the condition that approved key-recovery schemes be in place by 1999." [163]

Fair Use of Copyrighted Material on the Net

In *Religious Technology Center v. Lerma*, 1996 United States Dist. Lexis 15454 (E.D. Va. 1996), the Church of Scientology continued to prevail in its efforts to prevent copyrighted texts from being posted on the Internet. In the most recent case, the court rejected the defendant's analogies to the fair uses of "news gathering, scholarship, and time-shifting, and refused to extend any special fair use consideration to uses on the Internet." [164]

[163] "Export Granted for 56-Bit Encryption," *InfoSecurity* 8 (May 1997) 3:14.
[164] Biegel.

SUMMARY

- Legislators are honing laws to empower law enforcement and prosecutors to respond to criminal acts against the information infrastructure.
- Proposed legislation indicates a desire on the part of the legislators for continued enhancement of the statutes in favor of protecting the information infrastructure, while ensuring the Constitutional rights of individuals.
- The UCMJ provides additional avenues of prosecution for computer-crime-related activities.
- The prosecution of Colonel James A. Maxwell, U.S. Air Force, demonstrates how an investigation can be begun by a civilian agency and prosecuted in a military court under charges that include the UCMJ.
- The case of Julio Cesar Ardita, an Argentinean resident, will never come to prosecution unless Ardita can be arrested in the United States. The United States does not have an extradition treaty with Argentina that covers computer crime.
- No law prohibits the DoD from using overt means to collect intelligence, or otherwise engaging in those activities necessary to support traditional military intelligence or counterintelligence missions.
- DoD activities are governed differently in times of war and peace, as is the DoD's role in the intelligence community.
- Operations personnel/system administrators are protected by statute in monitoring employer-owned systems, but some courts have held that an employee has a certain expectation of privacy in using an employer-owned system.
- Even though there have been several cases wherein the court held that an employee has no expectation of privacy in using an employer-owned system, warning banners and written policies are recommended to ensure that employees have been clearly advised of their rights.
- The next section addresses regulatory issues.

This page intentionally left blank.

SECTION 5

REGULATORY

This section updates the Regulatory Environment section of the 2nd edition. It builds upon the regulatory information provided in the 2nd edition and does not cover all regulations presented in the earlier edition; rather it is focused on recent events and current issues.

Over the last year, the regulatory community has implemented the *Telecommunications Act of 1996*; loosened encryption export restrictions; and in conjunction with other parts of the government, responded to Executive Order 13010, *Critical Infrastructure Protection* and Executive Order 13011, *Federal Information Technology*.

CONTENTS

In this section, regulations are defined as follows:

> Regulations are rules and guidelines established by administrative agencies that, if derived from statutes, may carry the force of law, such as the income tax codes. Congress created administrative agencies, such as the Internal Revenue Service, to establish and enforce regulations. Most Federal regulations are published in the Code of Federal Regulations. Regulations may apply to the general public, business entities, and the enforcing agency. States may create their own regulations. [165]

5.1 EXECUTIVE BRANCH

This section highlights information assurance-relevant Federal regulatory issuances, such as Executive Orders and Federal Regulations, which have come into force since 1 July 1996. The background, including relationships to legislation, and potential effect upon and significance to the engaged community will be discussed.

[165] Elias and Levinkind, *Legal Research,* pp. 6/40-41.

5.1.1 Executive Orders

Executive Order 13010, [166] ***Critical Infrastructure Protection***

Executive Order 13010, *Critical Infrastructure Protection*, was issued on 15 July 1996. It has been amended by Executive Order 13025, *Amendment to Executive Order 13010, The President's Commission on Critical Infrastructure Protection*, dated 13 November 1996, and Executive Order 13041, *Further Amendment to Executive Order 13010,* issued 3 April 1997. Committees established by the order include the Principals Committee, which reviews reports and recommendations before they are submitted to the President; an Advisory Committee of 15 Presidential appointees from the private sector; and the Infrastructure Protection Task Force (IPTF), which acts as a central clearing house for threat, vulnerability, and countermeasure information that relates to critical infrastructures. Exhibit 5-1-1 depicts the organization and membership of the PCCIP.

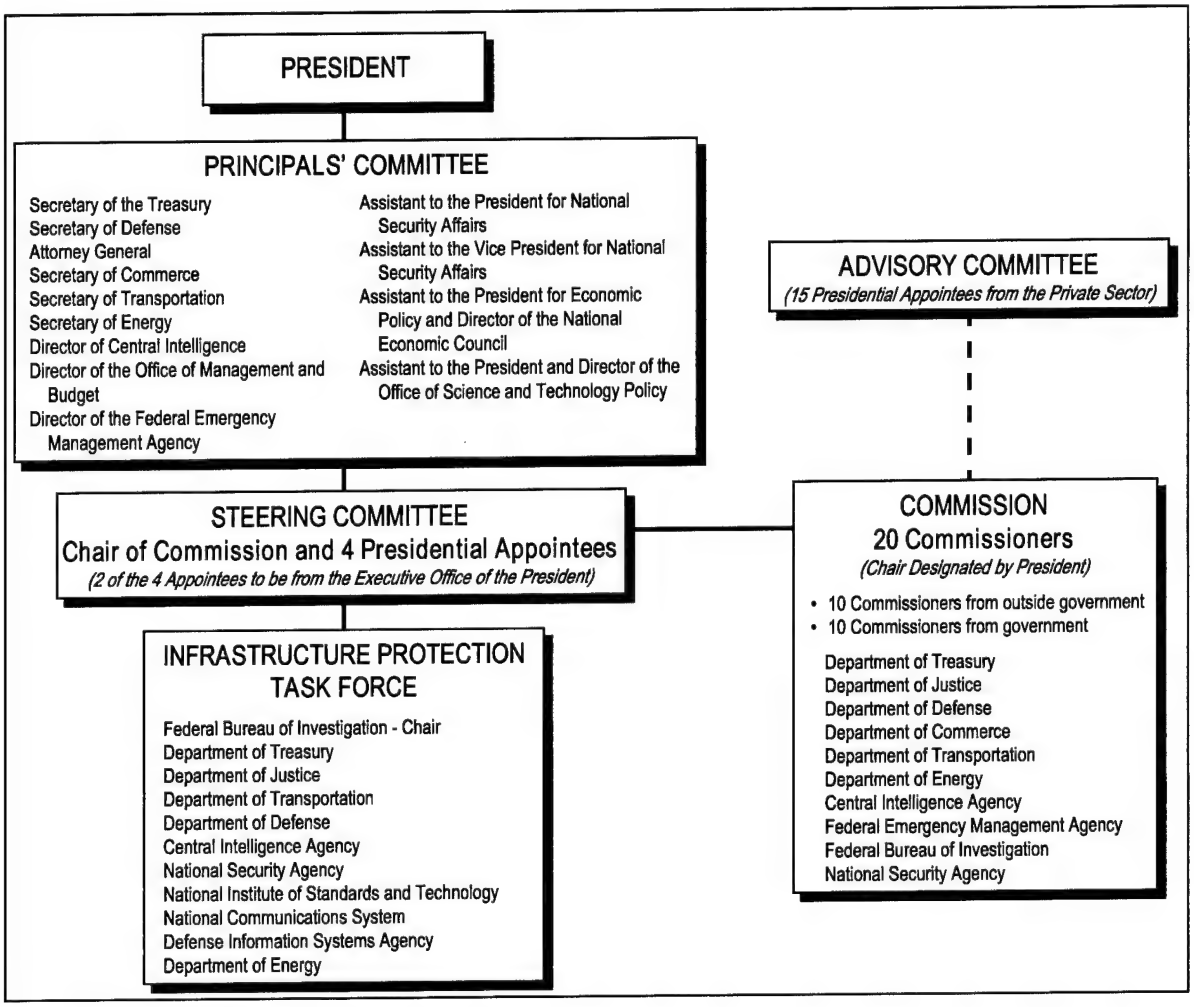


Exhibit 5-1-1. PCCIP Organization and Membership

[166] Executive Order 13010, *Critical Infrastructure Protection* (15 July 1996).

The general objectives of the PCCIP remain as set out in the original order, to:

- Identify and consult with public and private sector entities involved in infrastructure assurance; owners and operators of critical infrastructures; and others, including the Congress, who have an interest in critical infrastructure assurance and may offer differing perspectives on issues
- Assess the nature and scope of vulnerabilities and threats to critical infrastructures
- Determine legal and policy issues connected with critical infrastructure assurance and how to address them
- Recommend policy and strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation
- Propose statutory or regulatory changes needed to effect PCCIP recommendations
- Produce reports and recommendations to the Steering Committee as they become available, not limiting the reports to a final report.

The IPTF has already begun its work as the coordinator of threat, vulnerability, and countermeasure information for the U.S. Government, including all incidents that involve the information infrastructure. The purpose of the IPTF is to "increase coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact." The IPTF's function is to:

- Provide, facilitate, and/or coordinate expert guidance to critical infrastructures to detect, prevent, halt, or confine attacks, and to recover and restore service
- Issue threat and warning notices when advance notice of threats is received
- Provide training and education on methods of reducing vulnerabilities and responding to attacks
- Conduct after-action analyses to determine possible future threats, targets, or methods of attack
- Coordinate with law enforcement during or after an attack to facilitate criminal investigations.

The order specifies that all executive departments and agencies shall cooperate with the IPTF, providing assistance, information, and advice within the bounds of law. Finally, the order states that the IPTF shall terminate 180 days after the PCCIP terminates, unless extended by the President prior to that date.

The effect of the IPTF concept upon the U.S. Government's information assurance capability should be positive. There will be a single repository for incident statistics and other data, which should result in more realistic threat and vulnerability assessment, as well as better-targeted countermeasures. Having a central point of contact to distribute threat, vulnerability, and countermeasure information also should result in a more consistent state of preparedness Governmentwide.

Executive Order 12958, Designation Under Executive Order 12958 [167]

Executive Order 12958, *Classified National Security Information*, issued 17 April 1995, specifies that the President can designate officials with the authority to classify national security information. On 26 February 1997, President Clinton authorized the Chair of the PCCIP to originate classified documents at the Top Secret level for the period of time that the commission exists. The Chair may delegate this authority, according to section 1.4 (c) of Executive Order 12958. This order was necessary to enable the PCCIP to work with sensitive national security information.

Executive Order 13011, Federal Information Technology [168]

Executive Order 13011, *Federal Information Technology,* issued 16 July 1996, states that the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act* of 1996 provide the opportunity to significantly improve the way the Government acquires and manages information technology. To achieve this, the Order specifies that executive agencies of the U.S. Government shall:

- Implement the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996*
- Refocus their information management and acquisition processes to directly support their strategic missions, with a review process that ensures that budgets are being expended to an efficient and effective end
- Establish clear accountability for information resources management activities through Chief Information Officers (CIOs), who will participate in the investment review process, monitor and evaluate performance of information systems based upon applicable performance measures; and advise the head of agency when modification or termination of systems is warranted
- Cooperate to promote a "coordinated, interoperable, secure, and shared Governmentwide infrastructure," supported by diverse private sector supplies and well-trained information technology professionals
- Establish an interagency support structure that can provide expertise and advice to "enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

Heads of agencies are responsible for carrying out these activities within their own agencies. They are to enter into contracts for multi-agency acquisitions of information technology "if and in the manner that the Director of OMB considers it advantageous to do so."

---

[167] Executive Order 12958 *Classified National Security Information* (17 April 1995). White House Internet site, http://www.whitehouse.gov/

[168] Executive Order 13011, *Federal Information Technology* (17 July 1996). White House Internet site, http://www.whitehouse.gov/

The Order establishes three interagency organizations to aid OMB, the Departments of Commerce and State, and the General Services Administration in implementing the use of information technology. It sets out the purpose and functions of the Chief Information Officers (CIO) Council, [169] Government Information Technology Services (GITS) Board, [170] and the Information Technology Resources (ITR) Board. [171] Exhibit 5-1-2 summarizes the responsibilities of these entities.

ITRB	CIO Council	GITS Board
• Conducts independent assessment to aid in acquiring, developing, and managing selected major information systems. • Composed of U.S. Government IT practitioners with expertise in managing and developing major information systems. • Provides peer perspective on systems under review. • Provides recommendations to agency heads and OMB.	• Principal forum for U.S. Government coordination of Executive Order 13011. • Composed of CIOs and deputy CIOs of 28 executive agencies, as well as OMB representatives. • Identifies opportunities for cross-agency coordination. • Provides advice on IT strategy. • Assesses IT education and training needs.	• Ensures continued implementation of the IT recommendations of the National Performance Review. • Composed of agency representatives. • Consults experts on matters of concern. • Makes recommendations to the agencies, CIO Council, OMB. • Promotes development of innovative technologies, standards and practices.

Exhibit 5-1-2. Organizations Established by Executive Order 13011

The order also specifies that GSA will continue the FTS2000 long distance telecommunications service (provided by contract to the Federal Telecommunications Service (FTS)). Also, the Department of Commerce will carry out the standards responsibilities established by the *Computer Security Act of 1987*. The Department of State conducts liaison, consultation, and negotiations with foreign governments and foreign intergovernmental agencies and ensures that the United States participates in setting information technology standards in the international arena.

OMB has submitted a progress report, entitled *Getting Federal Computers Ready for 2000*, [172] which is aimed at assuring agency accountability in addressing the year 2000 computer problem. The report cites OMB Memorandum M-97-13, [173] which requires quarterly reports from U.S. Government agencies on the fifteenth of February, May, August, and November, 1997, and states that agencies in the Executive Branch have made good progress toward addressing the problem.

---

[169] See CIO Council Internet site, http://www.cio.fed.gov/

[170] See GITS Internet site, http://www.gits.fed.gov/

[171] See ITRB Internet site, http://www.gsa.gov/irms/ka/mka/itrb/

[172] U.S., Executive Office of the President, OMB, "Getting Federal Computers Ready for 2000" (15 May 1997). CIO Council Internet site, http://www.cio.fed.gov/yr2krev.htm

[173] Executive Office of the President, OMB, "Computer Difficulties Due to the Year 2000 - Progress Reports" (7 May 1997).

Executive Orders 13020 and 13026, Amendments to Executive Order 12924,[174] *Administration of Export Controls on Encryption Products*

Encryption has been a hotly contested topic. Executive Orders 13020, and 13026 were issued 15 November 196 as continuations of Executive Order 12924, *Administration of Export Controls on Encryption Products,* 19 August 1994. Until the 15 November 1996 order, encryption was defined as a munition and was regulated by the International Traffic in Arms Regulations (ITAR) and the *Arms Export Control Act* (AECA), which was administered by the U.S. Department of State. Encryption was subject to the controls of the U.S. Munitions List. The 15 November 1996 order transferred authority to regulate the export of non-military encryption to the U.S. Department of Commerce Bureau of Export Administration (BXA), to be regulated as a dual-use technology on the Commerce Control List (CCL) under the *Export Administration Regulations* (EAR), as are other export-controlled commercial products. [175]

A fuller discussion of the resulting regulation, which is codified in the *Code of Federal Regulations* (CFR), follows.

5.1.2 Federal Regulations

Export of Encryption

As stated above, non-military encryption is now regulated by EAR, 15 CFR Parts 730-774, which makes it illegal to export encryption software that exceeds 56-bit encoding. The new regulations allow the export of 56-bit DES, provided the exporter submits plans and demonstrates work in developing a key management structure that is consistent with Government specifications. The regulations also include procedures concerning the development of "a key management infrastructure." The most important of these is the creation of a license exemption that would allow "recoverable encryption products of any strength and key length to be exported freely after a single review by Commerce, Justice, and DoD." [176]

The new regulations expand the definition of products that are eligible for the key recovery license exemption, so that it includes "key escrow" systems, which use a trusted third party, as well as other systems, for recovery of keys or plain text. Self-escrow and escrowing of keys overseas under certain circumstances is allowed in order to make key recovery products more attractive in export markets. The Department of Commerce has developed pilot projects to demonstrate key recovery. [177]

---

[174] Executive Order 12924, *Administration of Export Controls on Encryption Products* (30 December 1996). White House Internet site, http://www.whitehouse.gov/

[175] U.S. Code of Federal Regulations, *Export Administration Regulations (EAR),* 15 CFR Parts 730-774 (7 January 1997).

[176] William A. Reinsch, "Administration Encryption Policy," testimony before the Subcommittee on International Economic Policy and Trade House Committee on International Relations, 8 May 1997. U.S. Department of Commerce, Bureau of Export Administration Internet site, http://www.bxa.doc.gov/warcong7.htm

[177] Ibid.

The National Institute of Standards and Technology has formed an industry advisory committee to develop requirements and standards for key recovery. The advisory committee has invited foreign government representatives to meetings to aid in ensuring coordination and compatibility on a multilateral basis. The President has appointed the U.S. ambassador to the Organization for Economic Cooperation and Development (OECD) as his Special Envoy on Encryption and has learned that several OECD countries have begun their own key recovery programs. [178]

In addition to setting out requirements for interoperability features and design, implementation, and operational assurance, Supplement No. 4 to Part 742 of the EAR, *Key Escrow or Key Recovery Products Criteria,* describes required key recovery feature as follows:

(1) The key(s) or other material/information required to decrypt ciphertext shall be accessible through a key recovery feature.

(2) The product's cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable by government officials under proper legal authority and without the cooperation or knowledge of the user.

(3) The output of the product shall automatically include, in an accessible format and with a reasonable frequency, the identity of the key recovery agent(s) and information sufficient for the key recovery agent(s) to identify the key(s) or other material/ information required to decrypt the ciphertext.

(4) The product's key recovery functions shall allow access to the key(s) or other material/information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.

(5) The product's key recovery functions shall allow for the recovery of all required decryption key(s) or other material/ information required to decrypt ciphertext during a period of authorized access without requiring repeated presentations of access authorization to the key recovery agent(s). [179]

Supplement No. 5 to EAR Part 742, *Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures*, describes the criteria the Department of Commerce will use in the export approval process. EAR Key Recovery Agent Requirements are:

(1)(a) A key recovery agent must identify by name, date, place of birth, and social security number, individual(s) who:

(i) Is/are directly involved in the escrowing of key(s) or other material/ information required to decrypt ciphertext; or

---

[178] Ibid.

[179] U.S. Department of Commerce, Bureau of Export Administration Internet site, http://www.bxa.doc.gov/supp4.htm

(ii) Have access to key(s) or other material/information required to decrypt ciphertext; or

(iii) Have access to information concerning requests for key(s) or other material/information required to decrypt ciphertext; or

(iv) Respond to requests for key(s) or other material/information required to decrypt ciphertext; or

(v) Is/are in control of the key recovery agent and have access or authority to obtain key(s) or other material/information required to decrypt ciphertext, and

(b) Must certify that such individual(s) meet the requirements of the following paragraphs (b)(i) or (b)(ii). BXA reserves the right to determine at any time the suitability and trustworthiness of such individual(s). Evidence of an individual's suitability and trustworthiness shall include:

(i) Information indicating that the individual(s):
(A) Has no criminal convictions of any kind or pending criminal charges of any kind;

(B) Has not breached fiduciary responsibilities (e.g., has not violated any surety or performance bonds); and

(C) Has favorable results of a credit check; or,

(ii) Information that the individual(s) has an active U.S. Government security clearance of Secret or higher, issued or updated within the last 5 years.

(2) The key recovery agent shall timely disclose to BXA when an individual no longer meets the requirements of paragraphs I.(1)(b)(i) or (ii).

(3) A key recovery agent must, to remain eligible for License Exception Key Management Infrastructure (KMI), identify to BXA by name, date, place of birth, and social security number any new individual(s) who will assume the responsibilities set forth in paragraph I.(1)(a) of this Supplement. Before that individual(s) assumes such responsibilities, the key recovery agent must certify to BXA that the individual(s) meets the criteria set forth in subparagraphs I.(1)(b)(i) or (b)(ii) of this Supplement. BXA reserves the right to determine at any time the suitability and trustworthiness of such personnel.

(4) If ownership or control of a key recovery agent is transferred, no export may take place under previously issued approvals until the successor key recovery agent complies with the criteria of this Supplement.

(5) Key recovery agents shall submit suitable evidence of the key recovery agent's corporate viability and financial responsibility (e.g., a certificate of good standing from the state of incorporation, credit reports, and errors/omissions insurance).

(6) Key recovery agents shall disclose to BXA any of the following which have occurred within the 10 years prior to the application:

(a) Federal or state felony convictions of the business;

(b) Material adverse civil fraud judgments or settlements; and

(c) Debarments from Federal, state, or local government contracting.

The applicant shall also timely disclose to BXA the occurrence of any of the foregoing during the use of License Exception KMI.

(7) Key recovery agent(s) shall designate an individual(s) to be the security and operations officer(s).

(8) A key recovery agent may be internal to a user's organization and may consist of one or more individuals. BXA may approve such key recovery agents if sufficient information is provided to demonstrate that appropriate safeguards will be employed in handling key recovery requests from government entities. These safeguards should ensure: the key recovery agent' structural independence from the rest of the organization; security; and confidentiality.

Supplement 5, Section II, *Security Policies*, sets out criteria aimed at ensuring the confidentiality, integrity, and availability of the keys and other material required for decryption of the ciphertext. Supplement 5, Section III, *Key Recovery Procedures,* states that key recovery agents must be designed to maintain the capability to make needed information available to decrypt within two hours of receipt of a request, maintain an audit trail of requests and responses, and have a back up/recovery system if the original system ceases to function properly or is deemed untrustworthy.

Enforcement and protective measures for export matters are codified at 15 CFR Part 764, which specifies conduct that constitutes a violation of the *Export Administration Act* (EAA) and/or the EAR. It sets out criminal sanctions through Federal court and other sanctions that are "neither administrative nor criminal." It identifies protective administrative measures that the BXA may take pursuant to its regulatory authority. [180]

According to the BXA, criminal penalties for knowing violations of the EAR include a fine of $50,000 or five times the value of the exports involved, whichever is greater, and or imprisonment. Administrative sanctions may also be imposed. These include revocation of

[180] 15 CFR Part 764, Sec. 764.1.

validated export licenses; general denial of export privileges; exclusion from practice; and/or fines of up to $10,000 per violation, or for a violation of national security export controls, $100,000. The maximum civil penalty allowed by law during periods in which regulations are continued by Executive Order, pursuant to the *International Economic Emergency Powers Act* (IEEPA), is $10,000 per violation. [181]

The Assistant Secretary for Export Enforcement also can issue Temporary Denial Orders, which deny any or all export privileges of a company or individual to prevent an imminent export control violation. Such orders deny the right to export from the United States, but also the right to receive or participate in exports from the United States. [182]

Section 11(h) of the *Export Administration Act* empowers the Secretary of Commerce to revoke any export license a party has at the time of a conviction. Section 11(h) also provides that, "at the discretion of the Secretary of Commerce, no person convicted of a violation of the EAA, IEEPA, or Section 38 of the *Arms Export Control Act* (or any regulation, license, or order issued under any of these laws) will be eligible to apply for or use any export license issued under the EAA for up to 10 years from the date of the conviction." [183]

The EAR does not prohibit the import of such technology, as long as the U.S. vendor took no part in its development and Sun Microsystems is planning to offer a Russian encryption product that provides 128-bit and triple DES encryption over the Internet. Sun will resell the product under the name PC SunScreen SKIP E+. SKIP E+ will support a variety of algorithms, including 56- and 64-bit DES, two- and three-key triple DES, and 128-bit codes. [184]

Sun did not seek government approval for the product and claims to have taken no part in its development. Sun is planning to provide the product to international offices of U.S.-based companies and others through third-party distributors. "SKIP E+ provides encryption and authentication of any IP-based communication, including Telnet, HTTP, SQL requests and SMTP, while it manages encryption keys, negotiates data transfers, and controls access to data through a three-tiered approval process. Sun has not yet completed work on creating a management model for the access lists that network administrators would need to create for a global system." [185]

---

[181] U.S. Department of Commerce, Bureau of Export Administration Internet site, http://www.bxa.doc.gov/eeprogrm.htm

[182] Ibid.

[183] Ibid.

[184] John Fontana, "Sun Crypto Skirts Feds," *Communications Week* (19 May 1997).

[185] Ibid.

5.2 OTHER REGULATORY AGENCIES

5.2.1 Federal Communications Commission

Since the passage of the *Telecommunications Act of 1996*, the FCC has taken on many new responsibilities. The act is drastically changing the rules for competition and regulation in most sectors of the communications industry, including local and long-distance telephone services and cable television, as well as broadcasting and equipment manufacturing. It was designed to increase competition in America's communications industry. The act places much of the responsibility for implementation on the FCC, while respecting state authority over the bi-lateral agreements that the incumbent local exchange carriers (ILECs) must reach with each new qualified entrant.

The FCC regulates, licenses and monitors the operation of communications services to ensure competitive nationwide and international communications. The services regulated include broadcast (radio and television), telephone, wireless (cellular, PCS, satellite), and other digital and analog applications. Transmission facilities include radio, wire, cable, light-guide, and satellite.

The following is the breakdown of FCC information-assurance related offices, along with their responsibilities, which provide context in understanding the FCC's role in implementing the *Telecommunications Act of 1996*.

- The Common Carrier Bureau handles domestic wireline telephony.
- The Mass Media Bureau regulates television and radio broadcasts.
- The Wireless Bureau oversees wireless services, such as private radio, cellular telephone, personal communications service (PCS), and pagers.
- The Cable Services Bureau regulates cable television and related services.
- The International Bureau regulates international and satellite communications.
- The Compliance & Information Bureau investigates violations and answers questions.
- The Office of Engineering & Technology (OET) evaluates technologies and equipment. [186] The OET also supports the FCC's federal advisory council, known as the Network Reliability and Interoperability Council (NRIC) which addresses FCC Standards and planning roles, granted by section 256 of the *Act*. [187]

5.2.2 Implementing the *Telecommunications Act of 1996*

The *Telecommunications Act of 1996* directs the FCC to aid in expanding competition in communications. A major task is to open up local telephone markets to new competitors. These new competitors are now called the "competitive local exchange carriers" (CLEC) by the FCC

[186] FCC Internet site, http://www.fcc.gov/bureaus.html
[187] FCC Internet site, http://www.fcc.gov/oet

and Alternate Local Exchange Carriers or ALECs by State Commissions, while the incumbent LEC, such as the RBOCs, GTE, SNET, Frontier, Cincinnati Bell, and many of the 2,000 independent telephone companies across the United States, are defined by the FCC as the ILECs and local exchange carriers (LECs) by the States. The FCC has worked with state commissioners to revamp regulations to bring them in line with the *Telecommunications Act*. The work was divided into three major areas: interconnection, universal service, and access charge reform. [188]

The *Act* requires that ILECs provide interconnection and unbundled network elements at reasonable rates. In fact, in the interest of fostering competition, the act requires that ILECs sell their services to CLECs at wholesale rates. The FCC has adopted rules for interconnection, timely disclosure of changes to ILEC networks, and pricing of ILEC services provided to CLECs. The goal of this regulation is to allow "communications traffic to pass between networks freely and transparently." [189] Several ILECs challenged certain provisions of the FCC interconnection orders and its authority to set prices in Federal court. A recent decision of the 8th Circuit U.S. Court of Appeals overturned these provisions. The FCC and its Commissioners see the court's actions as a delay in the realization of open market competition. [190]

The *Telecommunications Act* codifies the concept of achieving universal service, that is, affordable service for all Americans. The FCC is working with a board of state commissions to bring about a universal service system that fits within the "procompetitive, de-regulatory national policy framework" required by the act. Now competitors to local telephone companies can receive universal service support from a Federal fund. The FCC has set a schedule to implement universal service funding by 1 January 1999. [191]

Finally, the FCC has been working toward ensuring that access charges (the fees that Long Distance or Interexchange Carriers (IXCs) pay the LECs for delivering and originating calls over their respective networks) are reasonable. The goal is to ensure that access charges reflect the actual cost of providing access. [192]

5.2.3 FCC Local and State Government Advisory Committee

The FCC's Local and State Government Advisory Committee advises the FCC concerning impact decisions that the *Telecommunications Act of 1996* have or may have on local and state governments. The first meeting of the 14 advisors was held on 18 April 1997.

Among the issues discussed at the meeting were: "tower siting: new challenges facing local zoning authorities and the FCC with the rapid build-out of PCS and digital television; public

---

[188] Rachelle B. Chong, "Interesting Times at the FCC," Remarks of FCC Commissioner Chong at the University of California at Berkeley, 27 June 1997. Federal Communications Commission Internet site, http://www.fcc.gov/Speeches/Chong/sprbc707.html

[189] Ibid.

[190] Susan Ness, FCC Press Release, ÒRegarding Judicial Ruling on Interconnection Rules" (18 July 1997). U.S. FCC Internet site, http://www.fcc.gov/Speeches/Ness/States/sn-th

[191] Chong, op. cit.

[192] Chong, op. cit.

rights-of-way: how best to reconcile the needs of local governments to manage the use of their public-rights-of-way with the pro-competitive thrust of the *Telecommunications Act of 1996*; and over-the-air-reception devices: how the FCC's rules work and suggestions for improvements or modifications." [193]

5.2.4 Federal Advisory Committees

The FCC receives input and recommendations from its telecommunications-related Federal Advisory Committee, currently known as the (NRIC) Network Reliability and Interoperability Council, which was established following the massive service outages of the PSN in the early 90s. The NRIC's final report on interconnection contains a number of IA-related recommendations for the PSN. The Council's report was presented to the FCC on 15 July 1997 [194] In essence, the NRIC's recommendations have established the expectations, rules, and potential outcomes for each industry participant in the new open market local exchange telecommunications environment. [195]

5.2.5 Spectrum Management

FCC Chairman Reed E. Hundt has stated that his two main goals are: "to increase competition in communications and to ensure that all Americans share in the benefits of the communications revolution." [196]

The FCC's New Spectrum Policy has four basic principles:

- Competition, not monopoly, in all uses of the airwaves
- Flexible use of the airwaves for commercial purposes
- Clearly defined guidelines for all uses of the airwaves that are not strictly commercial (i.e., public interest uses)
- The award of licenses through competitive, quantifiable, open, and fair processes."

Current policies have lifted a Government ban on more than two companies holding licenses to provide fully mobile telephone service. The restriction was lifted because it had resulted in a duopoly with no incentive to promote competition. In addition, the FCC has begun auctions to sell licenses. This is a change from the comparative hearing process of the 1930s through the 1970s, and the lotteries of the 1980s. Auctions result in licenses being granted within months rather than years, thus allowing new technologies to enter the marketplace more rapidly.

---

[193] FCC Internet site, http://www.fcc.gov/state&local

[194] FCC Internet site, http:/www.fcc.gov/oet/nric/

[195] Minutes Of The 20 May 1997 Meeting of The Network Reliability and Interoperability Council. FCC Internet site, http//www.fcc.gov/oet/info/orgs/nric/meetings/m970520.html

[196] Reed E. Hundt, "Spectrum Policy and Auctions: What's Right, What's Left," Remarks to Citizens for a Sound Economy, Washington, D.C., 18 June 1997. FCC Internet site, http://www.FCC.gov/Speeches/Hundt/spreh734.htm

In future legislation concerning FCC auctions, the FCC will push for considering the following:

- That auctions be used to allocate all spectrum, except for public safety agency use and international allocation
- That Congress set no timetable for auctioning new spectrum licenses
- That maximizing auction revenues never be considered in setting spectrum policy
- That it is not necessary to impose equipment standards, channel loading rules, efficiency standards, or similar performance requirements when flexible spectrum licenses are awarded through auctions
- That auction winners pay for the license at the time of award so that the FCC does not have to act as a debt collection agency.

Transfer of Certain DoD Radio Frequencies to Non-Defense Use

A recent report by the General Accounting Office [197] states that the planned transfer of selected parts of the radio frequency spectrum may adversely affect important military communications systems and joint/multi-service tactical operations in the field.

The *Omnibus Budget Reconciliation Act* (1993) requires the Federal Government to provide a span of frequencies totaling no less than 200 megahertz (MHz) for allocation to the public. The intent of Congress was to promote new telecommunications products and services. However, the act stipulates that the frequencies allocated to public use must not be "required for the present or identifiable future needs of the Federal Government" and should not result in cost to the Government exceeding the benefits to be gained. In 1995, the National Telecommunications and Information Administration (NTIA) identified some 235 MHz of Government spectrum for transfer, including 50 MHz from within the U.S. Navy's Cooperative Engagement Capability (CEC) band. (The CEC originated as an improvement to Navy ship air defense.) If the transfer takes place, the Navy may have to set up guard bands of 75 MHz each on both sides of the 50 MHz to protect non-defense systems from potential radio frequency interference. To implement the guard bands, the military would have to give up, not only the original 50 MHz, but also another 150 MHz of guard bands, for a total of up to 200 MHz from the band currently in use by the CEC. According to the GAO, DoD is concerned that the loss of up to 200 MHz to non-DoD users could prevent CEC from functioning in a joint environment or against tactical ballistic missiles. According to the GAO, the full DoD-wide cost and operational impacts from the frequency transfer have not been identified.

In addition, the Air Force might have to transfer certain test range frequencies, which could delay the timely progress of important aircraft development. The Air Force also anticipates problems in high-power air defense radar operations, which may be caused by the loss of

---

[197] GAO. Report to Congressional Committees GAO/NSIAD-97131 *Defense Communications: Federal Frequency Spectrum Sale Could Impair Military Operations* (June 1997).

frequencies now used as guard bands. Loss of the guard bands would, in effect, move civilian systems closer to the radar frequencies and increase the likelihood of interference.

The FCC has completed a rule-making action to allocate the first 25 MHz from the CEC band to the General Wireless Communication Service. The GAO report advised "it is prudent to consider a delay in the reallocation process until the results of an ongoing comprehensive DoD spectrum study are available." According to GAO, a "critical problem for DoD is identification of frequencies needed to support new information warfare requirements." Contributing to DoD's problems, says GAO, is a DoD spectrum management responsibility that is "fragmented and inadequate." GAO notes that while the Joint Spectrum Center was set up in 1994 to consolidate spectrum management, these activities were "deconsolidated" in 1995 because the Military Services wanted to retain their own frequency management offices.

5.2.6 Anticipated Regulations

Foreign Participation in the U.S. Telecommunications Market

In June 1997, the FCC released a Notice of Proposed Rulemaking on foreign participation in the U.S. telecommunications market. [198] The notice proposes a policy that would "liberalize entry into the U.S. telecommunications market for most foreign-affiliated carriers. The notice anticipates that the liberalization will ensue when the WTO agreement on basic telecommunications services takes effect on 1 January 1998. The agreement promises to open 95 percent of the world's telecommunications market to U.S. companies and, as a reciprocal measure, the United States will open its own market to WTO member nations. The FCC intends to retain certain safeguards, such as the authority to deny or condition foreign carrier entry if it is in the public interest.

In agreeing to the WTO accord, 65 nations, including the United States, pledged to uphold the "Reference Paper on Pro-Competitive Regulatory Principles, which contains a binding, enforceable set of competition rules. These rules include guarantees of fair and economical interconnection between competing carriers; prohibitions on anticompetitive conduct; and independent regulation of the telecommunications industry. These pro-competitive rules incorporate principles that are at the heart of the *Telecommunications Act*, and contain an effective dispute resolution mechanism to allow full enforcement by WTO members." [199]

Foreign carriers have been allowed to buy into the U.S. market, on a restricted basis, since 1995. The FCC notice states, however, that the rules under which foreign investment has been allowed are burdensome and not in the best interest of the public. The FCC has concluded that it is no longer necessary to carry out the detailed analyses conducted in the past. The FCC will view favorably 100 percent indirect foreign ownership of common carrier radio licensees, as long as the applicants are WTO members. The FCC also has concluded "that it is no longer necessary to

---

[198] FCC, Commission Action, "Commission Initiates Proceeding to Review Rules and Policies on Foreign Participation in the U.S. Telecommunications Market, 4 June 1997. FCC Internet site, http://www.fcc.gov/Daily_Releases/Daily_Business/1997/db970605/nrin7019.html

[199] Ibid.

apply an equivalency analysis as the basis for authorizing carriers to provide switched services over resold or facilities-based private lines between the United States and WTO member countries." [200] The FCC also proposes not to apply the test for "cable landing licenses for submarine cables between the United States and other WTO countries." [201] The FCC does intend to retain the existing test for Section 214, Title III, and cable landing license applications from non-WTO members, but not to determine whether to permit U.S. carriers to enter into "alternative settlement arrangements with carriers from WTO member countries under its Flexibility Order." [202] The FCC proposes to require prior approval to add circuits on affiliated routes and to require carriers to file quarterly circuit status reports. Finally, the notice requests comments as to whether the FCC should require a "level of structural separation between a U.S. carrier and a dominant foreign affiliate, and asks for comment on what that level of separation should be." [203]

Domestic-International Satellite Consideration Order II

In January of 1996, the FCC issued *Domestic-International Satellite Consideration Order* (DISCO), which allows all U.S.-licensed satellites to offer domestic and international services. On 14 May 1996, the FCC released a *Notice of Proposed Rulemaking*, dubbed DISCO II, which proposes allowing foreign satellite systems access to the U.S. satellite services market. On 18 July 1997, the FCC issued FCC 97-252, *Further Notice of Proposed Rulemaking, In the Matter of Amendment of the Commission's Regulatory Policies to Allow Non-U.S.-Licensed Space Stations to Provide Domestic and International Satellite Service in the United States and Amendment of Section 25.131 of the Commission's Rules and Regulations to Eliminate the Licensing Requirement for Certain International Receive-Only Earth Stations and COMMUNICATIONS SATELLITE CORPORATION Request for Waiver of Section 25.131(j)(1) of the Commission's Rules As It Applies to Services Provided via the INTELSAT K Satellite.* [204]

FCC 97-252 cites the WTO Basic Telecom Agreement and asks for comment on the best way to promotes a competitive satellite market in the United States by allowing non-U.S. satellites into the United States. The notice defines a non-U.S. satellite as one that does not hold a commercial space station license from the FCC, while a U.S. satellite is a commercial space station licensed by the FCC. [205]

The notice states that 49 countries, including the United States, have made commitments to open satellite services to competition under the WTO agreement. It describes these commitments as

---

[200] FCC, "Commission Initiates."
[201] Ibid.
[202] Ibid.
[203] Ibid.
[204] FCC, FCC 97-252, "Further Notice of Proposed Rulemaking, In the Matter of Amendment of the Commission's Regulatory Policies to Allow Non-U.S.-Licensed Space Stations to Provide Domestic and International Satellite Service in the United States and Amendment of Section 25.131 of the Commission's Rules and Regulations to Eliminate the Licensing Requirement for Certain International Receive-Only Earth Stations and COMMUNICATIONS SATELLITE CORPORATION Request for Waiver of Section 25.131(j)(1) of the Commission's Rules As It Applies to Services Provided via the INTELSAT K Satellite" (18 July 1997).
[205] Ibid., p. 4.

involving the mobile satellite services and fixed-satellite services that do not involve one-way satellite television and radio services. [206] Similar to how it proposed liberalizing the telecommunications market, the FCC proposes to promote competition by dropping the analysis that is currently applied for non-U.S. satellites to enter the United States when the satellite is licensed by a WTO member nation. The FCC proposes to retain the analysis for non-WTO members, intergovernmental organizations, and services for which the United States has taken an exemption from most-favored-nation obligations under the WTO Basic Telecom Agreement ("non-covered services"). [207] The notice states that the U.S. "has taken an exemption from most-favored-nation obligations for one-way transmission of direct-to-home (DTH) television service, direct-broadcast satellite (DBS) television service, and of digital audio service." [208] The FCC does propose to retain the right to deny licenses when the license would not be serving the public interest.

In a separate statement, Commissioner Rachelle B. Chong emphasized "that it is not the goal of this proceeding to create unnecessary regulations or an overly restrictive framework for analyzing applications. Rather, we seek ways to foster a robust, competitive, worldwide market for satellite services." [209]

The FCC noted the WTO Basic Telecom Agreement will have "unprecedented impact worldwide in opening basic telecommunications markets to competition." [210] The FCC also pointed out that landlines may be used in place of certain global communications systems, such as mobile satellite systems; and that a landline call could actually reach its destination before a satellite connection occurred. [211]

FCC 97-252 states that the FCC would want to confirm that satellite markets will actually open to the U.S. before issuing any licenses; and will consider "guidance from the Executive Branch when appropriate; any other public interest concerns relevant to the decision to permit access by non-U.S. systems, including the significance of the proposed entry to the promotion of competition in the United States and the global satellite service market; issues of national security, law enforcement, foreign policy, and trade policy; and issues of spectrum availability and coordination." [212] In the notice, the FCC puts forth the idea of entering into bi-lateral agreements and states that DISCO II objectives will not be met by licensing satellites operated by intergovernmental satellite organizations or those engaged in services for which the U.S. has taken a most-favored-nation exemption from the WTO Basic Telecom Agreement, because this would not alter the competitive environment.

---

[206] Ibid., p. 9.
[207] Ibid., p. 4.
[208] Ibid., p. 4.
[209] Rachelle B. Chong, Statement "Amendment of the Commission's Regulatory Policies to Allow Non-U.S.-Licensed Space to Provide Domestic and International Satellite Service in the United States (DISCO 96-111; CC. Doc. No. 93-23; File No. ISP-92-007)" (17 July 1997). FCC Internet site, http://www.fcc.gov/Daily_Releases/Daily_Business/1997/db970717/discorc.txt
[210] "Further Notice."
[211] Ibid., p. 5.
[212] Ibid., p. 6.

SUMMARY

- Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP).
- The PCCIP Infrastructure Protection Task Force (IPTF), chaired by the FBI, acts as a central clearing house for critical infrastructure threat, vulnerability, and countermeasure information.
- Executive Order 13011, *Federal Information Technology,* combined certain goals of the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act* of 1996 to significantly improve the way the Government acquires and manages information technology, including multi-agency acquisitions of information technology.
- Executive Order 13011 established clear accountability for information resources management activities through Chief Information Officers (CIOs) in Federal Government agencies and established a CIO Council.
- New encryption regulations allow the export of 56-DES encryption, provided the exporter submits plans and demonstrates work in developing a key management structure consistent with Government specifications.
- Such encryption export is now regulated by the Department of Commerce, rather than the Department of Defense.
- The Federal Communications Commission (FCC) oversees the implementation of the *Telecommunications Act of 1996* and in so doing, has established an FCC Local and State Government Advisory Committee, as well as a Federal Advisory Council.
- A major task in expanding competition in communications as the act demands, is to open up local telephone markets to new competitors.
- A parallel task involves auctioning off spectrum.
- The FCC has announced DISCO II, which proposes allowing foreign satellite systems access to the U.S. satellite services market.
- The general atmosphere of opening up telecommunications markets worldwide is discussed in Section 6, International Aspects of Information Assurance.

SECTION 6

INTERNATIONAL ASPECTS OF INFORMATION ASSURANCE

This section addresses international organizations that are engaged in information assurance activities and the issues they are addressing. It begins with a discussion of the Global Information Infrastructure (GII), then summarizes some of the most significant topics. The rest of the section contains the details of specific organizations, and their purpose, as well as their major information assurance-related initiatives and documents. It is important to note that a range of entities are "placing a marker" in the GII arena, including financial, legal, and trade organizations.

CONTENTS

6.1 THE GLOBAL INFORMATION INFRASTRUCTURE

The reliability of the GII depends upon the actions of individual nations and groups of nations, and the United States is a leader in promoting a strong GII. The United States participates as a member of international organizations that are prominent in developing national and international information infrastructures, as well as the policies and laws under which they operate. It should be noted, however, that the international organizations discussed herein do not assume the power of a sovereign state in imposing policy, regulations, and law. Member states in such organizations choose to abide by agreements, but domestic laws and interests of the individual states can still be asserted, and the international organization has little recourse in the matter. Thus, expecting consistency in the international arena is problematic.

The United States is active in a number of international organizations, promoting policies and standards to encourage wide public access to information systems, while protecting the privacy

of individuals, national interests, and the ability of law enforcement to combat computer-related crime. However, the gap between information infrastructures in developing and highly industrialized nations remains large. The thrust of most international organizations is to lessen this gap, while promoting the economic interests of their respective member states and organizations.

The World Bank describes developing economies as: the newly industrialized states of the former Soviet Union, Eastern Europe, and Central Asia; Latin America and the Caribbean; Sub-Saharan Africa, the Middle East, and North Africa; South Asia, East Asia, and the Pacific. It believes that, even though developing nations may not appear to have use for the type of information infrastructure required in more developed nations, information technology can "create unprecedented possibilities for sustainable economic development, just as it has for business in the industrial world. . . Fortunately, the information revolution creates both the challenge and the means necessary for successful adjustment. It also creates new possibilities to attack vexing problems of poverty, inequality, and environmental degradation with the potential to achieve unprecedented gains in economic and human development." [213]

Information infrastructure concerns of the highly industrialized nations tend toward facilitating economic growth, protecting privacy of citizens, protecting national interests, preventing crime, and establishing standards. To an extent, the decisions these nations make may affect the United States' ability to ensure consistency in its international information services due to the multilateral nature of U.S. corporate entities and the interconnectivity of communications and financial systems. The United States' 1996 *Telecommunication Act* seeks to ensure the opportunity for free competition, fairness, and adequate enforcement within the U.S. telecommunications industry. The United States has promulgated these ideals through its strong support of international agreements, such as the World Trade Organization's (WTO) 1997 *Basic Telecommunications Services Agreement* and the 1995 *Information Technology Agreement,* which reduce tariffs, establish pro-competitive regulation, and open information technology markets in over 90 percent of the WTO's 130 member nations. When the *Basic Telecommunications Services Agreement* is fully implemented (by 1 January 1998), U.S. corporations will have the opportunity to establish a presence in foreign nations and to acquire, in whole or in part, ownership of foreign telecommunications companies. In this way, the United States may be able to help ensure the availability of information services by eliminating the need to use undesirable systems. The agreement also opens the door for foreign entities to operate in the United States and acquire ownership of U.S. corporations. [214]

The discussion that follows presents an overview of information assurance issues and activities in the international arena, beginning with major international organizations that are actively addressing information assurance. Included are pertinent documents published by each. The work of individual countries is not addressed, as this would be too cumbersome. Next is a brief summary of international perspectives on issues of privacy, encryption, and standards, as well as

---

[213] Philip Gaudette and Eduardo Talero, "Harnessing Information for Development: A Proposal for a World Bank Group Strategy," The World Bank (1 April 1996) on the World Bank Internet site, http://www.worldbank.org/html/fpd/harnessing/hid2.html

[214] Charlene Barshefsky, "Statement" (15 February 1997).

security, computer crime, and cooperation in multi-national jurisdictions. The notes include a bibliography, as well as on-line resources and membership lists for the international organizations.

Summary of Information Assurance Issues

The following is a summary of major international information assurance issues by topic.

- **Privacy.** In 1980, the Organization for Economic Co-operation and Development (OECD) developed and adopted a set of voluntary privacy guidelines that were accepted by its member countries. In 1981, the Council of Europe, whose membership consists of the European Union (EU) adopted "fair information practices" similar to those of the OECD to regulate the collection, storage, and automated processing of personal data and transborder data flow. The OECD and Council of Europe privacy guidelines provide a framework for domestic legislation for member and non-member nations and recognize diverse means of protecting information privacy, including self-regulation and industry codes of conduct. The *North American Free Trade Agreement* (NAFTA) and the *General Agreement on Trade in Services* (GATS) Annex on Telecommunications also contain provisions that recognize national privacy protection regulations. [215] In addition, the European Parliament *Directive 95/46/EC* lays out a set of guidelines for EU member states to follow in protecting the privacy of their citizens.

- **Encryption.** The International Organization for Standardization (ISO) has issued standards on encryption. On 27 March 1997, the OECD adopted its *Guidelines for Cryptography Policy,* which sets out principles for countries to follow in formulating policies and legislation on the use of cryptography. The guidelines encourage the use of cryptography for data protection and commercial applications, but recognize law enforcement and national security interests. The OECD recommends in this document that governments remove, or avoid creating unjustified obstacles to trade in the name of cryptography policy and that governments coordinate national policies at the international level. The EU has officially recognized the need for encrypted broadcasts, such as cable and pay-per-view television, and certain EU members, such as France, have begun to loosen regulation of lower-level encryption for private persons. The Bank for International Settlements (BIS) published *Implications for Central Banks of the Development of Electronic Money,* 1996, and *Security of Electronic Money,* August 1988, which address issues surrounding electronic money, including such security issues as cryptography.

- **Information Security Policies and Actions.** The ISO and the OECD have both written guidelines for nations to use in securing information systems. These are publicly available. The United States participated in writing these documents to propagate good

[215] Department of Commerce, Information Infrastructure Task Force, "The Global Information Infrastructure: Agenda for Cooperation" (February 1995).

and consistent security practices that will ensure the privacy rights of individuals in international commerce.

The implementation of the *Telecommunications Act* will result in networks of networks to replace monopoly carriers. Another result may be hundreds of companies having a hand in networks where there was once one. It is not yet known how this will affect the United States' ability to ensure system security. Another unknown is the impact of implementing the *Basic Telecommunications Services Agreement*, which will allow U.S. corporations to establish a presence in foreign nations and to acquire, in whole or in part, ownership of foreign telecommunications companies, and will also allow foreign interests to operate in the United States and acquire ownership of U.S. corporations. The percentage of critical systems that rely upon commercial lines makes this a significant factor to monitor and evaluate.

- **International Law.** The United States has entered into numerous bilateral treaties and agreements that enable international exchanges and mutual legal assistance in the apprehension and prosecution of persons involved in information system-related crimes. In practice, the United States can count on cooperation only in so far as it serves the national interests of the foreign country involved. For example, many countries refuse to allow extradition of a person who will be subject to the death penalty. The United Nations' *Model Treaty on Extradition* is representative of the kinds of terms commonly negotiated into extradition treaties. The U.N. example requires that extraditable offenses be punishable under the laws of both parties by imprisonment, deprivation of liberty, or a more severe punishment. It specifies mandatory refusal if the offense for which extradition is requested is regarded as a political offense. What the United States regards as terrorism and espionage fall into this category under the laws of some countries. The UN model also specifies mandatory refusal to extradite if the request concerns an offense under military law that is not also an offense under criminal law. Optional grounds for refusal include when the person whose extradition is requested is a national of the requested state. [216]

  The OECD *Guidelines for the Security of Information Systems* recognizes growing information system-related crime among its members. It calls for member nations to adopt criminal and civil sanctions against such crime and for mutual legal assistance and extradition in matters related to information systems. European Union Recommendations (89) 9 and (95) 13 address computer crime and problems of criminal procedural law connected with information technology.

- **Standards.** The major problem that arises from standards in information technology is that the speed with which technology develops often outpaces the establishment of standards for the same technologies. Consistency in practice is a major factor in assuring the availability, integrity, and confidentiality of information systems. A major question is how vulnerable lack of consistency may leave future systems that will developed in this environment of deregulation and privatization.

---

[216] See *Model Treaty* at United Nations Crime and Justice Information Network Internet site, http://www.ifs.univie.ac.at:80/~uncjin/unrule17.html

ISO is the leader in establishing international standards for information systems and related technologies. Because a major purpose of the EU is to further the economic development of Europe as a whole, system interoperability is a topic of great importance, as well as security, privacy, and transaction verification and authentication in banking. Pursuant to these concerns, the European Commission issued its communication, *Standardization and the Global Information Society: the European Approach.* The OECD *Guidelines for the Security of Information Systems* specifically stresses the need for "worldwide harmonization of standards."

6.2 INTERNATIONAL ORGANIZATIONS ACTIVE IN INFORMATION ASSURANCE

This section gives the details of information infrastructure assurance activities conducted by major international organizations. Each organization is introduced before its information infrastructure activities are discussed to give context to the significance of the information infrastructure activities. The National Telecommunications and Information Administration assisted in verifying the information presented herein.

6.2.1 NATO

NATO was established on 17 September 1949, with the purpose of promoting mutual defense and cooperation among its members. The alliance consists of 16 independent member countries, including the United States. Its 16 members include: Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and United States.

The North Atlantic Cooperation Council (NACC), an extension of NATO, was established on 8 November 1991 to discuss cooperation on mutual political and security issues. Its 43 members include: Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Kazakstan, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Tajikistan, Turkey, Turkmenistan, Ukraine, United Kingdom, United States, and Uzbekistan.

The NATO Science Committee has initiated programs aimed at enhancing the communications infrastructure available to the scientific and technological communities within Cooperation Partner countries (members of NACC). These include providing advanced networking workshops, linkage grants, and networking infrastructure grants.

NATO conducts two kinds of workshops: policy and training. Policy workshops aim at harmonizing network policies at the national and international levels to provide a stronger basis for collaboration between Cooperation Partners and NATO countries. This type of workshop brings together users and policymakers for coordination in planning and developing research

networks. Training workshops are used to transfer advanced technical knowledge to network administrators.
Linkage Grants are reciprocal visits of research teams. With the goal of improving communication between teams, NATO encourages Linkage Grant holders to consider whether upgrading Cooperation Partners' networking equipment will strengthen the quality and quantity of exchanges. Pursuant to this, NATO offers Supplements for Computer Networking to purchase small equipment, such as modems, software, and leased line service fees and subscriptions. NATO also offers Networking Infrastructure Grants to Cooperating Partners, to promote local and international cooperation in establishing links and networking capabilities. Such grants are provided primarily for equipment to improve telecommunications facilities. These infrastructure projects are regional by definition and aimed at upgrading the general connectivity of a specific geographical region by providing increased bandwidth between major sites and distributing access to larger communities. [217]

6.2.2 European Union (EU)

The EU was founded on 7 February 1992. It evolved from the European Community to coordinate policy among its 15 members in the areas of economics and to establish a common market and currency, defense, justice, and other matters, such as improved living and working conditions. In general, the EU has been active in establishing policy and laws to bring its member states to closer cooperation in economic development, security, rights of individuals, and cooperation in criminal matters. EU community laws apply throughout the member states. [218]

The EU is based upon "three pillars," the first being the *Single Europe Act*, which seeks to join European nations as a community with common democratic institutions, a single currency, and central bank, as well as monetary and economic policy. The second pillar is a common foreign policy, with joint action and a common defense policy, based upon the Western European Union (WEU). The third pillar is closer cooperation in customs, police, and judicial matters. [219]

Important structural components of the EU include the European Parliament, an elected body of 626 members, who help draft, amend, and adopt European laws, and propose policy. Twenty representatives of member nations comprise the EU Commission, which proposes European legislation and actions, and oversees the implementation of common policies. The Council of the EU is composed of one minister from each of the member states for each topic (e.g., foreign affairs). The Council and Parliament adopt legislation that has been proposed by the Commission. Heads of the member states and the President of the Commission form the European Council, which meets once a year concerning broad lines for EU policy, and matters of foreign and security policy, as well as cooperation in justice and home affairs. [220]

The EU has been the focal point for European efforts to fortify and protect its information infrastructure. The EU claims a political responsibility for integrating its neighbors from Central and Eastern Europe, as well as the former Soviet Union and the Mediterranean. Two key issues

---

[217] NATO Internet site, http://www.nato.int/science/scope/cn.htm
[219] European Union Internet site, http://europa.eu.int/
[220] Ibid.

concerning the legal and regulatory aspects of information security within the EU are the differences in law of evidence among member states and regulations concerning trust as applied to information security. The EU participates in standards organizations and supports information technology competition policies.

The European Commission encompasses 24 Directorates-General (DG). The DGs involved in information assurance are:

- DG I (External Relations: Commercial Policy and Relations with North America, the Far East, Australia, and New Zealand)
- DG III (Industry)
- DG IV (Competition)
- DG X (Information, Communication, Culture, Audiovisual)
- DG XII (Science, Research, and Development)
- DG XIII (Telecommunications, Information Market, and Exploitation of Research)
- DG XV (Internal Market and Financial Services)
- DG XXI (Customs and Indirect Taxation)
- DG XXIII (Education, Training, and Youth)
- DG XXIV (Consumer Policy).

The two issues that concern all these DGs are the single currency for Europe, which includes electronic commerce, and the commitment of the EU to protecting data concerning individuals and their commercial transactions.

In 1994, the European Council issued an action plan for the information infrastructure of its member states and set up the Information Society Forum. Inaugurated on 13 July 1995, the 130-member Forum draws from all member states and represents the users of technology, such as industry and public services, social groups, content and service providers, network operators, equipment manufacturers, and institutions (members of the European Parliament, the Economic and Social Committee, and the Committee of the Regions). The Information Society Forum has published reports on EU social, cultural, political, and economic aspects of the Information Society. [221]

The European Commission's *Europe's Way to the Information Society: An Action Plan* was issued on 19 July 1994 in Corfu and among other things, set up the Information Society Forum. [222]

Directive 95 of the EC of the European Parliament and Council, *On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of*

[221] European Union Information Society Project Office Internet site, http://www.ispo.cec.be/
[222] European Union Information Society Project Office Internet site, http://www.ispo.cec.be/g7/back.html

Such Data states that members shall protect the individual citizen's right to privacy and shall not restrict the transmission of data across borders, except in cases of national security or criminal activity. European Council Recommendations (89) 9 and (95) 13 are the seminal directives on computer crime and procedural law as it pertains to information technology. (Note: recommendations are not binding on the member states.) Also, the *New Transatlantic Agenda: Joint U.S./European Union Action Plan*, 3 December 1995, addresses cooperation between the United States and EU on a range of issues, including information technology and information infrastructure topics.

6.2.3 Organization for Economic Co-operation and Development (OECD)

A successor to the Organisation for European Economic Co-operation (OEEC), which administered the U.S. Marshall Plan to reconstruct Europe, the OECD was established on 30 September 1961. The OECD's convention states it will promote policies designed to:

> achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus contribute to the development of the world economy; contribute to sound economic expansion in Member as well as non-Member countries in the process of economic development; and contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.[223]

Japan joined the OECD in 1964 and eight other countries have joined since then. The OECD's 29 members include the United States, Canada, Mexico, Australia, New Zealand, Japan, Iceland, and Turkey. European countries make up the rest of the membership. The EU is admitted as a special member. The OECD has no international legal powers and no budget for loans. Its purpose is to direct cooperation among the member states. The OECD provides a forum for member state collaborative efforts in approaching globalization of economic policy.

The OECD Information, Computer, and Communications Policy Committee has adopted policy recommendations concerning the global information infrastructure. The recommendations include statements on telecommunications issues, such as pricing of services, universal service obligations, and mobile and cellular communications. Among others adopted are recommendations addressing the economics of the information society, high performance computing and networking, the Internet, information technology standards, security, privacy, cryptography, and intellectual property rights. Current OECD efforts are directed toward establishing a global consensus and an international framework for privacy and individual autonomy (freedom of movement, freedom of assembly, and fundamental human rights) in the information infrastructure. [224]

---

[223] OECD Internet site, http://www.oecd.org/about/origins.htm

[224] OECD Internet site, http://www.oecd.org/

The President has appointed the U.S. Ambassador to OECD as his Special Envoy on Encryption and has found that several OECD countries have begun their own key recovery programs.[225]

The OECD's *Recommendation of the Council Concerning Guidelines for Cryptography Policy,* 27 March 1997, identifies issues that should be taken into consideration in formulating cryptography policies at the national and international level. *Guidelines for the Security of Information Systems*, 26 November 1992, address the international nature of information systems and their worldwide proliferation, as well as the need to establish safeguards to ensure service. Guidelines include protection of privacy and securing information systems. The OECD *Declaration on Transborder Data Flows,* 11 April 1985, and the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980, seek to protect the right of the individual to control personal data and its use.

6.2.4 Group of Seven Nations (G7)

The G7, comprised of the United States, Canada, Italy, France, Germany, Japan, and the United Kingdom, was established on 22 September 1985. The G7 aims at facilitating economic cooperation among its members, including electronic commerce. Although normally a gathering of government representatives only, the G7 has begun to consult with private industry on topics concerning the information infrastructure.

The G7 has established "eight core principles" to realize the common vision of G7 nations for the global information infrastructure. These principles are:

- Promoting dynamic competition
- Encouraging private investment
- Defining an adaptable regulatory framework
- Providing open access to networks
- Ensuring universal provision of and access to services
- Promoting equality of opportunity to the citizen
- Promoting diversity of content, including cultural and linguistic diversity
- Recognizing the necessity of worldwide cooperation with particular attention to less developed countries. [226]

The G7 desires to promote interconnectivity and interoperability; develop global markets for networks, services, and applications, ensure privacy and data security; protect intellectual property rights; cooperate in R&D and in developing new applications; and monitoring social and societal implications of the information society.

---

[225] William A. Reinsch, "Administration Encryption Policy" (8 May 1997).
[226] European Union Information Society Project Office Internet site, http:www.ispo.cec.be/g7/keydocs/themepap.html

The G7 has held two pertinent conferences: The Information Society and Development Conference, held in May of 1996, and the G7 Information Society Ministerial Conference, held in February of 1995. Since the Ministerial Conference, the G7 and the European Commission have been pursuing 11 pilot projects in a range of areas. These are:

- Global Inventory
- Global Interoperability for Broadband Networks
- Cross-Cultural Training and Education
- Electronic Libraries
- Electronic Museums and Galleries
- Environment and Natural Resources Management
- Global Emergency Management
- Global Healthcare Applications
- Government Online
- Global Marketplace for Small and Medium Sized Enterprises
- Maritime Information Systems.

The Global Inventory Project provides an Internet-based multimedia inventory of information regarding national and international projects, studies, and other data relating to the information society. The Global Interoperability for Broadband Networks Project is attempting to ensure global interconnectivity and interoperability of high-speed test-beds and broadband networks. The Maritime Information Systems Project (MARIS) is creating global electronic navigation charts to prevent marine environmental disasters; a logistics information network for real-time information on cargo and vessels; a worldwide fisheries and oceans information network to provide better information on fish stock management; and a project for intelligent manufacturing of ships interlinking shipyards and their suppliers and customers in a common global network.[227]

The G7 is heavily involved in issues of electronic commerce and banking through its Financial Action Task Force (FATF), the international body most active in addressing money laundering in international banking. FATF has established its *40 Recommendations* that are the framework for virtually all anti-money laundering programs in the international community today. One of these recommendations is to constantly review emerging information technologies for their potential impact upon financial crime.[228]

---

[227] European Union Information Society Project Office Internet site, http://www.ispo.cec.be/g7/g7main.html and Keith Chang, "G7 Information Society Pilot Projects: An Overview and the Current Status," presented at the EITC '96, Brussels, (25-27 November 1996).

[228] Department of Treasury Financial Crimes Enforcement Network Internet site, http://www.ustreas.gov/treasury/bureaus/fincen/40rec.pdf

6.2.5 Organization of American States (OAS)

OAS is the world's oldest regional organization. It dates from the First International Conference of American States, held in Washington, D.C., October 1889 to April 1890. There are currently 35 OAS member states, with 37 Permanent Observers and the EU. The purpose of the OAS is to: strengthen peace and security in the region; promote democracy while maintaining a policy of non-intervention; prevent conflict, and failing that, seek peaceful resolution of conflicts; provide unified action in the face of aggression; promote cooperation; and limit conventional weapons, thereby freeing money to meet humanitarian needs. Other major OAS issues include promoting free trade, combating crime, and promoting technical cooperation among the member states. [229]

The Telecommunications sector is one of the most important items on the international agenda. The OAS recognizes that information infrastructure issues must be resolved to allow its member states to compete in the international arena and to raise the quality of life for its citizens. OAS has charged the Inter-American Telecommunications Commission (CITEL) with identifying and meeting telecommunications needs for member states.

CITEL has three Permanent Consultative Committees (PCC). These address public telecommunication services, broadcasting, and radio communications. Working groups of the Public Telecommunication Services PCC address legal matters, standards, basic and universal telephone services, network modernization, and tariffs. Working groups of the Broadcasting PCC concern digital audio broadcasting and coordination of incompatibilities with the 1981 Rio de Janeiro Plan; while the Radio communications PCC working groups are interested in very small aperture terminals in the Americas; terrestrial mobile communications; implementation of low earth orbit satellite system service below 1 GHZ in the Americas; and international radio amateur permits. Within the PCCs, two joint working groups concern the use of the radio spectrum and preparations for future International Telecommunication Union conferences.

CITEL plays a pivotal role in implementing the OAS *Declaration of Principles and Plan of Action for the Americas,* derived from the meeting of senior telecommunication officials on 25 - 26 September 1996. The plan concerns strengthening information infrastructures in the region for the purposes of economic, social, and cultural development. [230]

OAS also has published a pamphlet concerning CITEL's mission and activities entitled, *CITEL: Inter-American Telecommunication Commission.*

6.2.6 Asia-Pacific Economic Cooperation (APEC)

APEC was established in 1989 to promote trade and investment in the Pacific basin. Its membership has included the United States, Canada, Mexico, Chile, People's Republic of China, Hong Kong, Japan, South Korea, Mexico, and Chinese Taipai. The Association of Southeast Asian Nations (ASEAN), the Pacific Economic Cooperation Conference, and the South Pacific

---

[229] Organization of American States Internet site, http://www.oas.org/EN/PINFO/OAS/oas.htm

[230] Organization of American States Internet site, gopher://oasunix1.oas.org:70/0R0-3727-pub/english/resolut/gen_assm/yr95/agd1315.txt

Forum are observers to APEC. These countries represent a little less than half of the world's total merchandise trade. APEC has formed the Pacific Economic Cooperation Council, which is composed of governmental, academic, and business representatives, and the Business Advisory Council, which seeks to increase private sector participation in policymaking. [231]

Among the Asia Pacific Information Infrastructure's (APII) stated goals are ensuring the protection of intellectual property rights, privacy, and data security; creating a flexible policy and regulatory framework; encouraging business/private sector investment and participation; and narrowing the infrastructure gap between the advanced and developing economies. APEC's Working Group on Telecommunications provides a forum for members to exchange information, consult on policy and regulatory developments and standards, and to develop projects in their common interest. It is organized into steering groups, including Business Facilitation, which has two information infrastructure project groups: Data Compilation and Electronic Commerce. While the Electronic Commerce project group focuses on topics pertinent to electronic commerce, the Data Compilation group addresses wider initiatives among APEC member states, such as promoting standards information sharing and spectrum access, as well as exchanging, compiling, and disseminating telecommunications infrastructure and regulatory information.

APEC's Working Group on Telecommunications has published: (1) *The State of Telecommunications Infrastructure and Regulatory Environment of APEC Economies* (July 1996), (2) *The Seoul Declaration on Asia Pacific Information Infrastructure*, 1995, and (3) documents on communications policy issues associated with electronic data interchange and electronic commerce. [232]

6.2.7 International Telecommunication Union (ITU)

The ITU was founded in Paris in 1865 under the name International Telegraph Union. On 9 December 1934, the name was changed to the International Telecommunication Union, and in 1947 it became the United Nations' specialized agency that deals with world telecommunications issues. There are 187 ITU member states, including the United States, and 363 members from scientific and industrial companies, public and private operators, broadcasters, and regional/international organizations. The purpose of the ITU is to provide a forum for public and private sector cooperation in developing telecommunications. The ITU adopts international regulations and treaties that govern terrestrial and space uses of the frequency spectrum, and develops standards to facilitate interconnection of telecommunication systems on a worldwide scale. The ITU has, in fact, been working to promote international cooperation in the field of telecommunications longer than the United Nations has been in existence.

The ITU's mission covers three domains: technical, development, and policy. The technical domain promotes the development and efficient operation of telecommunications facilities; the development domain offers technical assistance to developing nations; and the policy domain works at the international level to promote a broader approach to the issues of

---

[231] APEC Internet site, http://www.apecsec.org.sg/apecnewinfo.html
[232] Ibid.

telecommunications in the global information economy and society. Its current ITU structure encompasses Radio communications, Standardization, and Development Sectors, as well as a General Secretariat. [233]

The Radio Communications Sector seeks to ensure equitable and efficient use of the radio-frequency spectrum by all radio communication services, including geostationary-satellite orbit. The Telecommunications Standardization Sector studies technical, operating, and tariff questions. It issues recommendations worldwide concerning its findings. The Telecommunication Development Sector discharges the ITU's responsibility as a U.N. specialized agency and an executing agency for implementing U.N. projects. The Sector's goal is to facilitate and enhance global telecommunications development through technical cooperation and assistance activities.

Though the ITU is known for setting standards in radio and telecommunications, in 1992, the Plenipotentiary Conference expanded the ITU's mandate, as documented in Article One of its constitution. Article One describes an additional purpose of the ITU as:

> to promote at the international level, the adoption of a broader approach to the issues of telecommunications in the global information economy and society, by cooperating with other world and regional inter-governmental organizations and those non-governmental organizations concerned with telecommunications. [234]

Pursuant to this, the ITU is assembling information to aid developing countries in restructuring their telecommunication sectors, and has convened several regulatory colloquia where experts from different countries discuss topics, such as interconnection in the context of competing infrastructure providers, universal services, telecommunications, and trade. The ITU also has launched a survey of the regulatory status of telecommunications sectors in various countries to determine the extent to which privatization, deregulation, and competition have been adopted. ITU radio conferences have made significant radio frequency allocations to enable the establishment of communications from any one point to any other point on Earth. In addition, the ITU is collaborating with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in standardization for the global information infrastructure.

At the first World Telecommunication Development Conference, held in March 1994, Vice President Al Gore introduced five principles as the foundation for global cooperation. These are:

- Encouraging private sector investment
- Promoting competition
- Providing open access to the network for all information providers and users
- Creating a flexible regulatory environment that can keep pace with rapid technological and market changes

[233] ITU Internet site, http://www.itu.int/aboutitu/whatitu.html
[234] Ibid.

- Ensuring universal service. [235]

Members of the ITU incorporated these principles into the ITU's *Buenos Aires Declaration on Global Telecommunication Development for the 21st Century*. (The Information Infrastructure Task Force, chaired by the Secretary of the Department of Commerce, published *The Information Infrastructure: Agenda for Cooperation*, which elaborates upon Vice President Gore's ideas and outlines a plan of action for the international community's use in enacting the five principles.) [236]

The ITU implements the February 1997 WTO telecommunications agreement. Also, the ITU has presented a *Memorandum of Understanding to Facilitate the Free Circulation of Global Mobile Personal Communications by Satellite User Terminals*, which has been adopted by 88 members.

The 1995 *Buenos Aires Declaration* states that "the development of telecommunications may be fostered by liberalization, private investment, and competition in appropriate circumstances." It suggests that their introduction in any restructuring exercise should be compatible with national development goals and with improving service to underserved areas. Such a restructuring should include a regulatory system that will:

> create a stable and transparent environment to attract investment; facilitate access of service providers to the network with a framework that promotes fair competition while protecting network integrity; ensure the provision of universal service, helping to achieve integrated rural development as well as promoting innovation and the introduction of new services and technologies; and guarantee the rights of users, operators and investors. [237]

6.2.8 International Organization for Standardization (ISO)

The ISO is a non-governmental organization that was established in February 1947 to promote the development of standards worldwide. It is composed of representatives of the national standards bodies of its members. The are 85 members, 26 correspondent members, and 9 subscriber members. The United States is a member. The ISO has been actively involved in setting standards for international usage in all aspects of the global information infrastructure, including electronic commerce and information system security. ("ISO" has been chosen as the name for the International Organization for Standardization rather than reference by a standard acronym. The name derives from the Greek word *iso*, meaning *equal*, which is the root of the prefix "*iso-*" that occurs in a host of terms, such as "isometric", "isonomy", etc.)

As a standards organization, ISO's publications are too numerous to list. A sample of information assurance-related documents includes: *Common Criteria for Information*

---

[235] Department of Commerce, Information Infrastructure Task Force, "The Global Information Infrastructure: Agenda for Cooperation" (February 1995). On U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) site on Internet at http://www.ntia.doc.gov/oiahome/giiagend.txt

[236] Ibid.

[237] ITU, *Buenos Aires Declaration on Global Telecommunication Development for the 21st Century* (1995).

Technology Security Evaluation (developed by the United States, France, Germany, the Netherlands, the United Kingdom, and Canada), a document divided into four parts: Introduction and General Model, Security Functional Requirements, Security Assurance Requirements, and Predefined Protection Profiles; and *Guidelines for the Management of IT Security (GMITS)*, which gives guidance on effective IT security management in three parts: Concepts and Models for IT Security, Managing and Planning IT Security, and Techniques for the Management of IT Security. ISO has published standards on login and password control, firewalls, digital signature and encryption, secure hash system/secure hash algorithm, and key certification and authentication, among many others. [238]

6.2.9 International Trade and Legal Organizations

The World Trade Organization (WTO)

The WTO, an organ of the United Nations, was established on 1 January 1995. The successor to the General Agreement on Tariffs and Trade (GATT), it is the institutional foundation of the multilateral trading system. Its main functions are:

- Administering and implementing the multilateral and plurilateral trade agreements that make up the WTO
- Acting as a forum for multilateral trade negotiations
- Seeking to resolve trade disputes
- Overseeing national trade policies
- Cooperating with other international institutions involved in global economic policy-making.

The WTO has 130 members, including the United States, with 29 governments currently under consideration for future membership. The Ministerial Conference, which meets every two years, is the highest WTO authority. Subsidiary bodies, such as the General Council, which also convenes as the Dispute Settlement Body and the Trade Policy Review Body, run the day-to-day business. [239]

On 15 February 1997, the WTO put forth the *Basic Telecommunications Services Agreement* to liberalize and deregulate the telecommunications market. It has been signed by 69 nations, which produce more than 90 percent of the world's telecommunications business. The agreement includes all forms of telecommunications and identifies the telecommunications infrastructure as the gateway to Internet growth. The proposed deregulation aims to promote competition by eliminating monopolies and stimulating private investment. It is an attempt to enable expansion of new uses of information technologies, such as electronic commerce and financial services. [240]

---

[238] International Organization for Standardization Internet site, http://www.iso.ch/
[239] WTO Internet site, http://www.wto.org/
[240] WTO Internet site, http://www.wto.org/wto/Whats_new/bt-summ3.htm and op. cit., Barshshevsky, 1997.

The Council for Trade-Related Aspects of Intellectual Property Rights monitors the operation of and compliance with the *WTO Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS), which provides protection and enforcement measures for intellectual property rights, including those related to software. [241] The WTO also has adopted the December 1996 Singapore *Ministerial Declaration on Trade in Information Technology Products,* which aims to eliminate tariffs on information technology products by the year 2000. [242]

To ensure that member nations receive equal treatment and protection, TRIPS incorporates the obligations of pre-existing conventions, such as the *Paris Convention for the Protection of Industrial Property* [243] and the *Berne Convention for the Protection of Literary and Artistic Works* [244] (copyright), and enhances the standards of protection set out in past documents. Included is a provision that computer programs be protected as literary works under the *Berne Convention.* TRIPS also outlines how databases should be protected. TRIPS states that authors of computer programs and producers of sound recordings have the right to authorize or prohibit commercial rental of their works to the public. Industrial designs are protected under the agreement for a period of 10 years, and the owners of the design can prevent the manufacture, sale, or importation of articles bearing or embodying a design that is a copy of the protected design. Rights apply to existing intellectual property, as well as new intellectual property. In addition, TRIPS provides a mechanism for multilateral dispute settlement.

United Nations Conference on Trade and Development (UNCTAD)

UNCTAD was established in December 1964 to promote international trade. Its membership includes all 188 UN members, plus the Holy See, Switzerland, and Tonga. UNCTAD's Trade and Development Board meets twice a year to discuss the

> international implications of macro-economic policies and issues concerning interdependence of economies and of problems and issues in the trade, monetary and financial fields, trade policies, and the problem of structural adjustment and economic reform. [245]

UNCTAD has four Standing Committees: Commodities, Poverty Alleviation, Economic Co-operation among Developing Countries, and Developing Service Sectors. Currently there are five Ad Hoc Working Groups, established for two years each: Investment and Financial Flows, Trade Efficiency, Privatization, Expansion of Trading Opportunities for Developing Countries, and Investment and Technology Transfer. UNCTAD also has responsibility for the UN's Economic and Social Council (ECOSOC), which includes the Commission on Transnational Corporations and its subsidiary body, the Intergovernmental Group of Experts on International

---

[241] International Trade Law Monitor Internet site, http://itl.irv.uit.no/trade_law/documents/freetrade/wta-4/art/iia1c.html

[242] WTO Internet site, http://www.wto.org/wto/Whats_new/inftech.htm

[243] Cornell University School of Law Internet site, gopher://gopher.law.cornell.edu:70/00/foreign/fletcher/

[244] Ibid.

[245] United Nations Conference on Trade and Development Internet site, http://www.unicc.org/unctad/en/aboutorg/works.htm

Standards of Accounting and Reporting, as well as the Commission on Science and Technology for Development. The Trade and Development Board is charged with reviewing progress in implementing the *Programme of Action for the Least Developed Countries (LDCs) for the 1990s.*

UNCTAD has adopted the position that hundreds of millions of dollars in transaction costs could be saved by using information technology in banking, insurance, customs, etc. [246] In 1994, UNCTAD held the UN International Symposium on Trade Efficiency (UNISTE) in Columbus, Ohio, which gathered international representatives from the government and private sectors to explore uses of information technology in expanding world trade. The Global Trade Point Network was launched at the Columbus conference. The network links over 50 points of trade in more than 30 countries.

United Nations Conference on International Trade Law (UNCITRAL)

UNCITRAL was formed in 1966 to address obstacles to trade that are caused by disparities in national laws. It has addressed issues such as electronic funds transfers, international bills of exchange and international promissory notes, and international credit transfers. UNCITRAL is composed of 36 member states, which are elected by the General Assembly. Membership is structured to fairly represent the world's geographic regions and all non-member states are invited to observe. Members serve 6-year terms, with the terms of half of the members expiring every 3 years. The United States' membership expires in 1998.

UNCITRAL has issued two model laws concerning transmission of data: *Draft Model Law on Electronic Commerce,* June 1996 and its predecessor, *Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication,* 1987. The draft on electronic commerce applies to data transmitted strictly for commercial purposes. It addresses digital signatures, acknowledgment of receipt, admissibility and evidential weight of data messages, and document retention. The 1996 model law provides standards by which to assess the legal value of electronic messages. To assist governments and courts in interpreting the model law, UNCITRAL also produced the *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* [247]

World Intellectual Property Organization (WIPO)

WIPO is a United Nations agency, established on 26 April 1970 to protect literary, artistic, and scientific works. It is one of the 16 specialized agencies of the United Nations. The United States is one of the 161 WIPO members.

WIPO administers two treaties: the *Paris Convention for the Protection of Industrial Property* of 1883 and the *Berne Convention for the Protection of Literary and Artistic Works* of 1886. [248] Intellectual property encompasses two main issues: industrial property, such as inventions, trademarks, industrial designs, and appellations of origin; and copyright, which pertains to

---

[246] Department of Commerce, "Report on International Organizations," by James A. Johnson (March 1997). On U.S. Department of Commerce NIST Internet site, nii.nist.gov/pubs/intl_org.html

[247] United Nations Internet site, http://www3.un.or.st/uncitral.commiss.geninfo.ht

[248] World Intellectual Property Organization Internet site, http://www.wipo.int/

literary, musical, artistic, photographic, and audiovisual works. WIPO's International Bureau is conducting a study on the international intellectual property issues of the global information infrastructure, including the Internet. WIPO has convened a panel of experts on trademarks and Internet domain names, and has a representative on the International Ad-Hoc Committee of the Internet Society, which is planning changes to the Internet domain name system. WIPO also is aiding developing countries in structuring intellectual property protection systems to meet the challenges of the information society. [249]

The United Nations Educational, Scientific, and Cultural Organization (UNESCO)

UNESCO, established on 16 November 1945, currently has 185 member states. The agency's aim is to promote cooperation in education, science, and culture. The United States is not a member of UNESCO. [250]

Because UNESCO historically has dealt with issues of copyright, intellectual property rights, and fair usage of information, it is now interested in the Internet and the global information society.

UNESCO conducted its first international conference on ethical, legal, and societal aspects of digital information in March of 1997. Topics included accessing digital information, universal access to information networks, intellectual property rights and information security, archiving digital information, and the accountability of information over time. UNESCO has no direct authority in these areas, but is in a position to influence the acceptance of information technologies in developing countries. "They believe they have a mandate to protect the ethical and societal and legal values impacted by the Internet." [251]

6.2.10 Satellite Communications Organizations

International Maritime Satellite Organization (INMARSAT)

INMARSAT was established in 1979 as an intergovernmental organization, providing worldwide communications for commercial, distress, and safety applications at sea, in the air, and on land. From its beginning as a pioneer in developing and providing maritime satellite communications, INMARSAT has grown to 75 members and operates the world's only global mobile satellite communications system. INMARSAT now provides a range of communications services for mobile and remote applications on land. Its fleet of satellites also carry flight deck, operational and passenger telephone, E-mail, and fax communications for most of the world's airlines. In 1995, it launched the world's first hand-portable global mobile satellite phone system, known as INMARSAT-phone. The demand for mobile telecommunications is on the rise. ICO, Iridium, Globalstar, and Odyssey also plan to offer personal mobile communications that will allow persons to travel from country to country and utilize the same mobile terminal. In March of 1997, INMARSAT members began to formally consider a move to a more commercial structure. A possible result is that in 1998, INMARSAT may undergo significant reform that would convert

[249] Department of Commerce, "Report on International Organizations," by James A. Johnson.
[250] UNESCO Internet site, http://www.unesco.org/general/eng/about/index.html
[251] Ibid.

it to a nationally registered limited liability company, which INMARSAT believes will provide a more flexible investment structure than is currently allowed. [252]
INMARSAT's satellites are in geostationary orbit, positioned to cover Earth in four ocean regions. There currently are three generations of satellites on orbit. With the evolution to the new structure, INMARSAT plans to diversify its business with the next generation of satellites to be launched circa 2001-2002. Also, under the new structure, INMARSAT's broad international ownership and participation will expand.

INMARSAT's basic document is the *Convention On The International Maritime Satellite Organization (INMARSAT) with Annex and Operating Agreement* (1976), as amended in 1985, with Protocol (1981). The treaty entered into force on 16 July 1979. [253]

International Telecommunications Satellite Organization (INTELSAT)

Founded in 1964, INTELSAT's purpose is to develop and operate a global commercial telecommunications satellite system. INTELSAT is an international not-for-profit cooperative comprised of 136 members. It is the world's largest commercial satellite communications services more than. Its global satellite system provides voice/data and video service to billions of people in more than 200 countries, territories, and dependencies throughout the world. Its owners contribute according to their use of the services, and any nation can use INTELSAT. The major customers are telecommunications operators, such as long distance telephone service providers and television broadcasters. Airlines, international banks, multinational manufacturers, and petroleum companies, as well as news and financial information services, also are major users, as is the United Nations. In 1995, INTELSAT demonstrated its satellites' capability to provide global access to the Internet. [254]

INTELSAT will augment its fleet of 24 spacecraft in geostationary orbit with the launch of six new satellites in 1997. INTELSAT's spacecraft are deployed to provide overlapping coverage to four regions: Atlantic Ocean, which covers the Americas, the Caribbean, Europe, the Middle East, India, and Africa; Indian Ocean, which serves Europe, Africa, Asia, the Middle East, India, and Australia; Asia Pacific, which encompasses Europe, Africa, Asia, the Middle East, India, and Australia; and Pacific Ocean, with coverage of Asia, Australia, the Pacific, and the Western part of North America.

INTELSAT is involved in a variety of information infrastructure activities. For example, INTELSAT establishes technical and operating standards for earth stations that connect with its systems. INTELSAT held the world's largest communications traffic planning meeting in Washington, D.C., 5 - 9 May 1997. This conference was attended by approximately 1,700 delegates representing more than 410 companies from 163 countries. The purpose of the meeting was to discuss satellite traffic plans to meet user needs for 1998 and beyond. INTELSAT participates in G7 conferences, including the 1996 Ministerial Conference on the Information Society and Developing Countries in South Africa, where it demonstrated extending an ISDN

---

[252] INMARSAT Internet site, http://www.inmarsat.org/inmarsat/low_bankd/html/media_supp/releases/start.txt
[253] ITU Internet site, http://222.itu.ch/itudoc/itu-r/cl/cm/cm2_32814.html
[254]INTELSAT Internet site, http://www.intelsat.int/cmc/info/intelsat.htm

network over satellite for PC-based videoconferencing. INTELSAT plans to introduce a dedicated business service to promote VSAT use for similar applications.

Representatives from 80 countries comprise INTELSAT's current management team. INTELSAT's basic document is the 12 February 1973 *Agreement Relating to the International Telecommunications Satellite Organization,* with its annexes and operating agreements. [255]

6.2.11 Banking Organizations Addressing Infrastructure Development and Electronic Commerce

World Bank Group (also known as the World Bank)

Established on 22 July 1944, the World Bank Group is a UN specialized agency providing economic development loans. The United States is one of the World Bank Group's 180 members. The World Bank Group is composed of the:

- International Bank for Reconstruction and Development (IBRD)
- International Development Association (IDA)
- International Finance Corporation (IFC)
- Multilateral Investment Guarantee Agency (MIGA)
- International Centre for Settlement of Investment Disputes (ICSID).

The IBRD is the World Bank Group's main lending organization. It was established in 1944 to lend money for development projects to "help governments change the way they manage their economies." [256]

The IBRD raises most of its funds on the world's financial markets by selling bonds and other debt securities to pension funds, insurance companies, corporations, other banks, and individuals around the world. The IDA was established in 1960 to assist the poorest developing nations. IDA loans are known as "credits" and are given to countries with annual per capita incomes of about $865 or less. Its fund is derived from government contributions, IBRD profits, and repayments on earlier IDA credits. The aim of the IFC, which was established in 1956, is to strengthen the private sector in developing nations; thus it lends directly to the private sector. About 80 percent of the IFC's funds are borrowed in international financial markets through public bond issues or private placements. The other 80 percent is borrowed from the IBRD. [257]

The purpose of MIGA, which was established in 1988, is to help developing countries attract foreign investment. "MIGA may insure up to 90 percent of an investment, with a current limit of $50 million per project." [258]

---

[255] Cornell University School of Law Internet site, gopher://gopher.law.cornell.edu:70/00/foreign/fletcher/BH585.txt
[256] World Bank Internet site, http://www.worldbank.org/html/extdr/glance.htm
[257] Ibid.
[258] Ibid.

Founded in 1966 to promote increased international investment "by providing facilities for the conciliation and arbitration of disputes between governments and foreign investors," the ICSID provides advice, conducts research, and publishes on topics of foreign investment law. [259] The World Bank Group is refocusing internal operations and external services to accommodate developments in information technology. [260] MIGA has sponsored seminars on monetary policy in an electronic environment. The Bank's InfoDev program has focused on developing infrastructure, as well as policies to encourage electronic commerce. The Bank regularly funds projects for modernizing banking systems in developing nations and participates in the Global Information Infrastructure Commission with the goal of bringing developing nations into the global information economy.

Ambassador Charlene Barshefsky, the U.S. Trade Representative, stated at the December 1996 WTO Ministerial Conference in Singapore that the World Bank estimates that the world's economies will demand U.S. $1.5 trillion over the next 10 years for "high quality infrastructure, advanced information technology, and telecommunications systems." [261] World Bank Group members will play a pivotal role in supplying and monitoring the use of these funds.

Inter-American Development Bank (IADB)

The IADB was established in December of 1959 to aid in accelerating economic and social development in Latin America and the Caribbean. It is the oldest and largest regional multilateral development institution. Per its charter, the bank's principal functions are to:

- Utilize its own capital, along with funds it raises in financial markets, as well as other available resources, to finance the development of borrowing member countries
- Supplement private investment when private capital is not available
- Provide technical assistance in preparing, financing, and implementing development plans and projects.

The 48 members of the IADB include the United States, Canada, nations of South and Central American, and the Caribbean, as well as Israel and certain European nations, such as Croatia, Slovenia, Sweden, Norway, Finland, France, Germany, and Denmark. The purpose of the IADB is to promote economic and social development in Latin America. [262]

The IADB launched its Informatics 2000 Initiative to restructure programs, in line with global developments in information technologies. The IADB is sponsoring online banking services through the Ministry of Posts and Telecommunications in Mexico, with a main goal of extending service in rural areas. The IADB will sponsor seminars for telecommunications and

---

[259] Ibid.
[260] Department of Commerce, "Report on International Organizations," by James A. Johnson.
[261] Charlene Barshefsky, Statement by the Honourable Charlene Barshefsky, Acting United States Trade Representative, World Trade Organization Ministerial Conference, December 1996.
[262] InterAmerican Development Bank Internet site, http://www.iadb.org/ENGLISH/ABOUTIDB/about_idb.html

policymaking officials to assist in implementing the WTO Agreement on telecommunications liberalization. The IADB is entering into an agreement with the Global Information Infrastructure Commission to co-sponsor events fostering broader awareness of the impact of information technologies. [263]

Bank for International Settlements (BIS)

The BIS was founded in January of 1930, and is owned and controlled by international central banks. It has 33 members, including the United States. BIS aims to promote cooperation among central banks in international financial settlements. A major goal of the BIS is to foster international financial stability. BIS promulgates meetings among the international central banks concerning "databank management, security automation, internal management procedures, the collection of international financial statistics, and specific legal topics of interest to central banks." [264]

As a service provider to the world's central banks, the BIS has an ongoing interest in electronic commerce and currencies. It also has a Euro-currency Standing Committee. The BIS published *Implications for Central Banks of the Development of Electronic Money,* 1996, and *Security of Electronic Money,* August 1988, which address issues surrounding electronic money, including such security issues as cryptography. [265]

6.2.12 Useful On-Line Resources for GII Topics

The Asia Pacific Economic Community (APEC) has two official sites: APEC Telecom Working Group at http://www.apec-wg.com/ and APEC Telecom Ministerial site at http://www.dca.gov.au/apec.html. The Government of Korea has created an Asia Pacific Information Infrastructure Cooperation Centre at http://www.apii.or.kr, and the Government of Japan hosts the APII Technology Centre at http://www.apii-tc.or.jp.

The Bank for International Settlements (BIS) site contains information concerning international electronic commerce initiatives and documents. It is located at http://www.bis.org/.

European Community (EU) official sites are: Europa, the EU's member-government on-line service, located at http://europa.eu.int/; and Information Society Forum at http://www.ispo.cec.be.

Group of Seven (G7) sites include the G7 Information Society, located at http:www.ispo.cec.be/g7/g7main.html. Details concerning the G7 1995 Information Society Conference are at http://ispo.cec.be/g7/particip.html, and 1996 ISAD Conference information is at http://www.csir.co.za/isad.

---

[263] Department of Commerce, "Report on International Organizations," by James A. Johnson.

[264] Bank for International Settlements Internet site, http://www.bis.org/about/index.htm

[265] Bank for International Settlements, "Security of Electronic Money, a Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries" (August 1996). On Bank for International Settlements Internet site at http://www.bis.org/publ/index.htm

The International Organization for Standardization (ISO) home page is located at http://www.iso.ch/. There is general information about organizational activities, with links to information about specific standards.

The International Telecommunications Union (ITU) home page is located at http://www.itu.int/. It contains information about the ITU, its activities, and documents.

The North Atlantic Treaty Organization (NATO) home page is located at http://www.nato.int/. Data concerning the Science Programme and Cooperation Partners can be found at http://www.nato.int/science/scope/cn.htm.

The Organization of American States (OAS) home page is located at http://www.oas.org/. Other sites include http://www.oas.org/EN/PINFO/nv7e.htm, which concerns telecommunications, and http://www.oas.org/EN/PROG/CITEL/citel.htm, which concerns CITEL.

The main site for the Organization for Economic Co-operation and Development (OECD) is http://www.oecd.org/. OECD Telecommunications and Information Services Policy working group site at http://www.oecd.fr/dsti/sti ict.html contains information infrastructure documents.

General information concerning and legal documents created by United Nations Conference on International Trade Law (UNCITRAL) can be obtained at http://www3.un.or.st/uncitral.commiss.geninfo.ht.

The World Bank Group home page is located at http://www.worldbank.org/.

The World Trade Organization (WTO) home page is at http://www.WTO.org/. This site contains background information and useful documentation.

Links that provide the U.S. perspective on international information infrastructure activities include the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) at http: www.ntia.doc.gov and NTIA's Office of International Affairs at http://www.ntia.doc.gov/oiahome/dianelist.html. Another significant U.S. site is the U.S. Trade Representative at http://www.ustr.gov/, which has links to agreements. The NIST is another useful site that contains general information and official documents. It is located at http://nii.nist.gov/.

SUMMARY

- International organizations involved in the GII do not assume the power of a sovereign state in imposing policy, regulations, and law.
- The United States promotes policies and standards to encourage wide public access to information systems, while protecting the privacy of individuals.
- NATO is aiding Cooperation Partner countries by providing advanced networking workshops, linkage grants, and networking infrastructure grants.
- The EU has been very active in attempting to smooth out standards, encryption, information security, and law enforcement issues among its member nations.
- The G7 has held several conferences and has begun 11 information technology/information infrastructure assurance projects.
- OAS considers telecommunications to be one of the most important items on the international agenda.
- APEC has been extremely active in information infrastructure enhancement and assurance.
- The ITU adopts international regulations and treaties that govern terrestrial and space uses of the frequency spectrum.
- ISO has developed the *Common Criteria for Information Technology Security Evaluation.*
- The WTO has put forth the powerful *Basic Telecommunications Services Agreement,* which has been signed by more than 69 nations including the United States.
- UNCTAD has adopted the position that millions of dollars in transaction costs could be saved by using information technology in banking, insurance, customs, etc..
- UNCITRAL has developed model laws for electronic commerce and extradition.
- UNESCO conducted its first international conference on ethical, legal, and societal aspects of digital information in March of 1997.
- INMARSAT provides a range of communications services for mobile and remote applications on land.
- The World Bank Group is financing information infrastructure development projects worldwide and is refocusing its internal operations and external services to accommodate developments in information technology.
- The IADB launched its Informatics 2000 Initiative to restructure programs in line with global developments in information technologies.
- BIS is a major player in electronic money and commerce, and in addressing cryptography issues.

SECTION 7

TECHNOLOGY

The purpose of this section is to explore some of the many technology issues that impact upon information assurance. While operational practice and law have a substantial influence on doctrine, these are all influenced in some respect by technological developments. With the speed of change in these areas it is necessary to highlight scientific findings, as well as noteworthy trends in research and development that are determining the issues. The potential effect upon warfighters and the significant impact upon the security of the Defense Information Infrastructure will be highlighted.

CONTENTS

7.1 OSD AND JOINT STAFF TECHNOLOGY INITIATIVES

The IA domain has benefited from recent initiatives of the Director, Defense Research and Engineering (DDR&E) and the Joint Staff to improve the responsiveness of the science and technology (S&T) community to warfighter requirements. Two related plans were developed by collaborative working groups made up of representatives from OSD, the Joint Staff, the Services, and Defense Agencies. These documents derive from *Joint Vision 2010* and are intended to focus the S&T community on developing technologies critical to joint warfighting capabilities. Both plans address near-, mid-, and long-term technology objectives, and will provide annual updates to maintain the necessary balance and focus in the S&T community.

The documents, which evolved in parallel, are the *Defense Technology Area Plan* (DTAP) [266] and the *Joint Warfighting Science and Technology Plan* (JWSTP). [267] The DTAP addresses technologies critical to the DoD acquisition community and the Services, and reflects the requirements of the JWSTP. The JWSTP will ensure that the S&T program addresses priority future joint warfighting capabilities. Both plans attempt to influence and integrate planned Advanced Technology Demonstrations (ATD) and Advanced Concept Technology Demonstrations (ACTD), conducted by the Services and Agencies.

---

[266] U.S. DoD, Director of Defense Research and Engineering, *Defense Technology Area Plan* (April 1996).
[267] U.S. DoD, Under Secretary of Defense for Acquisition and Technology, *Joint Warfighting Science and Technology Plan* (January 1996).

An example is the Joint Staff/J6 sponsored ACTD candidate, *Information Assurance: Automated Intrusion Detection Environment*, which seeks to demonstrate an integrated intrusion detection defense-in-depth capability. DISA has the lead on the ACTD, with STRATCOM as the primary participant. Other participants include TRANSCOM, DIA, DARPA, NSA, USAF, AFIWC, AFOSI, Rome Labs, CIA, DoJ, FBI, and industry. Planned for 3-year duration with a start in FY 98, the ACTD will develop an integrated environment and correlate sensor outputs over the first 2 years; it will add players and insert maturing technology every 6 months during the second and third years. At the conclusion, the ACTD will leave behind a deployed intrusion detection environment at up to 30 sites and most importantly, residual technical and operational links between the C4I and law enforcement intelligence and operations communities.

7.2 DARPA RESEARCH AND DEVELOPMENT

This section examines the major research and development community efforts impacting upon security and information assurance, viewed from both threats and protections. A key player in the community is the Defense Advanced Research Projects Agency (DARPA). Not only does DARPA engage in research, but it also sponsors numerous research efforts that address security either explicitly or implicitly. Four project areas are especially noteworthy: High Confidence Networking; High Confidence Computing Systems; Assurance and Integration; and Survivability and Vulnerability. Each of these four areas includes a significant range of projects. [268]

7.2.1 High Confidence Networking Research

The High Confidence Networking area is developing technologies which will become the basis for a networked communications infrastructure resistant to external and internal attack, even in an environment where the infrastructure supports wireless, mobile, and fixed location hosts. Interoperable solutions will be scaleable for global use in wide and local area networks.

Integrating authentication and other security mechanisms into routing, management, and directories will strengthen existing network infrastructures. The results will be additional programs to develop and use protocols that can detect and work around malicious attacks on the network infrastructure.

Value-added security services will be developed for use as part of the basic communications service. They may be integral, offered by third-party services, or packaged into libraries and toolkits for embedding security into applications. These security services will be designed to support broadcast and dynamic group (multicast) communications then will be used by higher-level services such as secure mail, real-time monitoring and intrusion detection, and electronic commerce.

---

[268] Detailed descriptions of the projects, including contractors and universities doing the research, can be explored in depth at http://www.darpa.mil

Technologies for key management infrastructures will support a wide range of cryptographic services and will allow interoperability of services across infrastructures. Common interfaces will allow the use of multiple cryptographic families.
Firewalls will use a combination of network-level and application-level controls to prevent exploitation of host, node, and network vulnerabilities. Distributed firewall technologies will also allow secure interaction between geographically-separated parts of an organization.

Network intrusion-detection technology will be developed that will be scaleable up to tens or even hundreds of thousands of nodes, will allow cooperation among intrusion-detection systems, will allow an automated adaptive response to attacks, and will be integrated with network management and diagnostic tools.

7.2.2 High Confidence Computing Systems Research

The High Confidence Computing Systems area is developing modular prototype systems with configurable, replaceable components for security, reliability, and real-time support.

Secure operating systems that can isolate suspect software and enforce locally-specified security policies are essential for distributed computing and cooperative problem-solving. The program develops modular prototype systems for high-assurance security and technologies to support dynamic, secure enclaves. These allow specific computing resources within a computer system to be assigned to and confined to specific security domains, even where these security domains may cross administrative boundaries.

Computing systems will provide the isolation needed to enforce the separation of enclaves and to allow untrusted processes (e.g., unexamined imported software) to be safely confined within end systems. Through appropriate definition of domains and permissions, these mechanisms will allow end-systems to enforce organization-specific security policies, including multilevel security. Security technology will be integrated with mainstream operating system research products. Systems will be designed for modular integration of a set of basic security services with readily removable and replaceable cryptography modules.

Hardware security is addressed through hardware verification of security-critical behavior of devices. Robustness is enhanced through the development of reusable trusted modules. These will provide standard interfaces, and offer order-of-magnitude cost improvements over existing fault-tolerant techniques. A new architecture will allow for secure, fault-tolerant real-time distributed systems.

7.2.3 Assurance and Integration Research

The Assurance and Integration program will develop tools for designing, integrating, and evaluating new systems for security and robustness. This area will develop tools for the development of trustworthy systems, as well as technology to allow developers to integrate distributed systems in a secure and robust way.

Middleware services will provide a set of mechanisms to handle transparently the secure synchronization of replicated objects, to secure reliable message passing, to provide redundancy management for fault tolerance, and to allow a distributed application to enforce a global set of policies. Techniques will be developed for the secure integration of data from heterogeneous sources, especially for Defense-relevant applications like distributed modeling and simulation.

Secure mediators will ensure that security is enforced during data exchange by performing label translations or controlling data aggregation. Tools for the development of trustworthy systems may include application of formal methods to demonstrate that software correctly enforces a security policy and to formally analyze policy interactions. These tools will build on methodologies, tools, and environments already under development to add reasoning about security and robustness properties. They will express modular system structures, networking, and other distributed services and protocols. Assurance technologies will integrate trusted system development techniques into standard system development environments. Security metrics, evaluation techniques, and testing tools will be developed to allow quantitative assessment of system security and/or strength against attack.

7.2.4 Survivability and Vulnerability Research

The Survivability and Vulnerability program will develop technologies for addressing vulnerabilities in the nation's computing infrastructure and emerging critical technologies that could be exploited by an information warfare enemy. These vulnerabilities are related to reliability, fault tolerance, timeliness, correctness, and their interaction with security mechanisms in the Defense/National computing infrastructure. This includes telecommunications, wireless communications networks, satellite systems, air traffic control systems, power distribution grid, oil and gas pipeline control systems, and other control systems. Contributing technologies are access controls, dependability design principles, assurance technologies, designs for improved survivability, evaluation techniques for measurable reliability, and management of interactions with security. Aspects of information warfare defense and attack scenarios will be included in wargaming simulations. Industry testbeds for technology demonstration will form part of a transition plan that will allow the current infrastructure to evolve to a more survivable one.

7.3 SEI SECURITY AND RISK MANAGEMENT ISSUES

Another major player in the security research and development arena, especially in the areas of software improvements and information security, has been the Software Engineering Institute (SEI). [269] The SEI is a Federally-funded research and development center at Carnegie Mellon University (Pittsburgh) that has made many significant accomplishments in the area of software productivity. In addition to reducing Defense software costs and increasing DoD efficiency, SEI has pursued studies of better ways to provide security and manage risk through:

- providing a focal point for identifying and countering risks to Internet security
- developing and transitioning more effective risk management practices.

[269] See http://www.sei.cmu.edu

The SEI Risk Program has worked with 27 Government and industry organizations to assess the software technical risk in 30 programs/projects:

- The SEI has provided a focal point for identifying and countering risks to Internet security. The Computer Emergency Response Team (CERT®) assisted in 2,897 security incidents by the end of 1993, preventing many millions of dollars in damages. The CERT® has issued about 100 advisories to the Internet community citing specific vulnerabilities and recommending appropriate corrective action.
- The SEI has developed a systematic risk identification method, which has been adopted by government and industry organizations as part of their risk management processes at division and corporate levels.
- DoD, Federal agencies, and commercial industry are initiating technical alliances to invest their funds and collaborate with the SEI on developing and testing risk management methods in acquisition and development.

There have been recent overtures for DARPA to discontinue funding for the CERT® Coordination Center, a facility run by the SEI. The rationale is: DARPA was established to provide management and funding for leading-edge research and development; the SEI is funded to improve DoD software quality and management processes; and the CERT® is already a proven concept with a real operational function. The intent is that another Defense agency or other Department should provide the management and funding of its activities; perhaps the commercial, industrial, and academic communities may want to underwrite its activities for common security values.

Another important research effort related to the CERT® was the recently published study of more than 4,000 security incidents on the Internet from 1989 through 1995. This most significant study was the doctoral dissertation of Dr. John Howard at Carnegie Mellon University. His work details characteristics of the Internet and why it has been subjected to an increasing number of security attacks. It explains the recordkeeping history and procedures of the CERT® and traces the evolution and development of different types of attacks on the Internet. [270]

7.4 THE INFOSEC RESEARCH COUNCIL

The INFOSEC Research Council (IRC) consists of U.S. Government sponsors of information security research from the DoD, Intelligence Community, and Federal Civil Agencies. The IRC provides its membership with a community-wide forum to discuss critical information security issues; convey the research needs of their respective communities; and describe current research initiatives and proposed courses of action for future research investments. Members obtain and share valuable information to help focus their information security research programs, identify

[270] John D. Howard, *An Analysis of Security Incidents on the Internet 1989-1995,* Dissertation, Carnegie Mellon University (7 April 1997). Available on Info-sec.com Internet site at http://www.info-sec.com/Internet/howard/Start.html

high-leverage, high-value research targets of opportunity, and minimize duplication of research. The IRC thus promotes intelligent information security research investments.

The IRC is still in the process of building its institutions for work, coordination, and collaboration. Three of the main areas for IRC work are: the INFOSEC Science and Technology Study Group, the Centers for INFOSEC Studies and Research, and the National INFOSEC Technical Baseline (NITB). With the Lawrence Livermore National Laboratory serving as the Executive Agent, the NITB collects information on the state of the national technical capability in critical INFOSEC areas. Focusing on the research community's key interests, it identifies the most difficult and challenging problems in need of further scientific explanation. Two of the key areas documented in its national repository of INFOSEC information are initiatives in intrusion detection and response, and the whole area of firewall technology. As an excellent illustration of its baseline effort, the NITB recently published a summary study that documented the history and capabilities of firewall technology. [271]

7.5 DISA INITIATIVES

The Defense Information Systems Agency (DISA) has initiated a number of managerial strategies for dealing with the challenges that rapidly evolving technology presents to Defense Information Warfare/Information Assurance goals. The most noteworthy include:

- *Creation of the Global Operation Security Center* (GOSC) for IW Management. This initiative will enable tracking of security problems and coordination of technology solutions. The continuation of this action will be the establishment of regional security centers, collocated with the DISA regional management centers.
- *Centralized Certification and Accreditation* of systems and networks. This initiative will ensure that certification and accreditation of technology is performed using a standard method.
- *Creation of the INFOSEC Program Management Office* (IPMO), with ties to NSA and DIA. This office: develops and implements the INFOSEC Management Program for DoD; provides operational protection, detection, and reaction capabilities in support of the Defense Information Infrastructure; executes DoD requirements and processes for certification of information systems and networks; manages the INFOSEC Technical Services Contract and the DoD-wide Antivirus Software Initiative.

7.6 NETWORK INTRUSION DETECTION ISSUES AND TECHNOLOGY

The following sections detail the varied problems/issues caused by intrusions into computer systems and the technologies that will aid administrators in detecting and preventing them.

---

[271] U.S. Department of Energy, Lawrence Livermore National Laboratory, *National INFOSEC Technical Baseline: Firewalls* (April 1997). On Internet at http://doe-is.llnl.gov/nitb/nitb.html

7.6.1 Network Intrusion Detection Issues

The Threat

The magnitude of the threat from various forms of intrusion, tampering, and malicious code was conveyed in testimony to a Senate committee investigating computer security. The suggestion was raised that about 120 countries are now working on developing an information warfare capability. With a view to the sophistication of many other countries in programming and Internet usage, the threat has to be viewed as a factor deserving much consideration. Over time, hacker tools have become easier to use, often requiring little or no technical expertise. For example, in the past year, programs have emerged from the hacker community that launch denial of service attacks or automate E-mail flooding. As these tools propagate, the threat to information systems increases as a larger threat population emerges with the technical capabilities once limited to a small portion of the hacker community. Exhibit 7-6-1 details some recent hacker activities.

Target System	Type of Attack
Department of Defense	Croatian teenage hacker used openly-available hacker tools to tap into the computers at Anderson Air Force Base.
CIA	WWW attack replaced the CIA home page with a protest page containing hacker links and pornography.
Department of Justice	WWW attack replaced the DoJ home page with a protest page featuring a picture of Hitler, hacker links and pornography. The attack potentially was spurned by the DoJ Supreme Court case over the *Communications Decency Act.*
U.S. Air Force	WWW attack replaced an Air Force home page with alternative content.
NASA	WWW attack replaced a NASA page with alternative content.
PANIX	Denial of Service SYN attack disrupted business operations for several days.
WebCom	Denial of Service SYN attack disrupted business operations for several days.
NCAA website	WWW attack replaced NCAA home page with racist content. This attack was coordinated to coincide with the announcement of the NCAA tournament selection committee results, thus maximizing the potential exposure of the hack.
British Labour Party website	WWW attack replaced Labour Party home page with alternative content.
Kriegsman Furs	WWW attack replaced corporate page with a protest page.

Exhibit 7-6-1. Recent Hacker Intrusions and Their Results

Software Tampering

Dan Farmer, the author of the famous Internet security testing program, the *Systems Administrators' Tool for Assessing Networks* (SATAN), released a utility for comparing operating systems against a known standard version to identify legitimate changes and unauthorized changes, perhaps containing viruses or Trojan Horse code.

Malicious Code

One of the more ominous findings has been that Java applets not only have various security weaknesses such as being able to perform undesired and destructive actions, but they can also compromise and attack firewall servers from the inside of the network.

Web Server Problems

Over the past year, numerous reports have been publicized of Web pages that have been altered by malicious intrusions. The most notable included unsavory messages that were posted as changes to the USAF and the CIA web pages. Another highly visible attack was the flooding of the White House E-mail system with Internet mailing lists; these were compounded by the autoresponder answering the mailing list postings. In another attack, a hacker known as "U4ea" planted swastikas and racist messages on the BerkshireNet in Pittsfield, Massachusetts, while erasing data on two computers and finally shutting down the system. In retaliation for articles about him, U4ea then attacked *The Boston Globe* computers and deleted its Web pages and those at the site, www.boston.net.

7.6.2 Intrusion Detection Technology

The DISA strategy for security management involves the three phases — protect, detect, and respond; for all three, it relies heavily upon the use of tools technology. Efforts to achieve this goal require capabilities being developed for: protection — vulnerability assessment tools; detection — audit monitoring and intrusion detection tools; and finally, reaction — malicious code detection and eradication tools. These general categories involve various products that are available on the commercial market as COTS products, as well as others being developed to meet unique Defense needs.

The major focus of the DISA effort in both intrusion detection and response is to enhance the security of the Defense Information Infrastructure (DII) and all of its components. Working in a cross-platform heterogeneous network, the various tools have to provide automated and continuous DII vulnerability analysis and response, especially by use of scheduled and on-demand probing, as well as long-term storage and manipulation of vulnerability information in a database accessible to those who need the data to respond (including software agents). The reporting and response capability should match the scope of operations and authority of DII center operations. A key power of these tools is the ability to provide automated and on-demand reports and notifications of intrusion and countermeasures taken.

As an essential part of the DII information assurance strategy to provide adequate protection and response against attacks, these security tools must complement and integrate with the network and system management tools found at the DISA Global, Regional, and Local Control Centers. Therefore, some of the requirements that the tools research and development also must meet include:

- *Continuous Background Operation.* The developed operations should operate continuously in a non-visible fashion.
- *Graphical User Interface.* System design should allow the user to effect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (menus, screens, buttons, etc.).
- *Hierarchical Capabilities.* Developed applications shall execute within the DII hierarchical structure as well as provide notification and reporting capabilities.
- *Modular.* The developed applications shall be constituted of separable modules.
- *Expandability.* The products shall be flexible and expandable to accommodate updates driven by newly identified attack and eradication methods.
- *Scalability.* The products shall have the ability to use the same application software on many different classes of hardware/software platforms, from personal computers to super computers.

In summary, these multi-layered information assurance tools will be interoperable and integrated with system and network management systems across the DII control hierarchy. They are an essential part of the DII information assurance strategy to ensure the confidentiality, integrity, and availability of Defense information. They will enable the constant security readiness of the DII and provide a realistic balance of proactive and reactive system security.

7.7 ENCRYPTION ISSUES

In addition to using tools to detect and respond to attacks, another way to deal with a range of problems involving data theft, information corruption and confidentiality, is encryption. The use of encryption has a long history in the military services as the classic guarantee of confidentiality, integrity, availability, authentication, and non-repudiation. Rapid changes in technology and continuously evolving threats to security have resulted in increased research in cryptographic measures. Not only does DoD have considerable research and development for newer and better encryption methods, but also industry and even organized crime have entered this old, but renewed, field. Newer and stronger types of encryption have been developed as methods of enhancing security, but new problems and issues, such as key escrow, have arisen.

7.7.1 Types of Encryption

There are two major types of encryption: symmetric and asymmetric. They are detailed in the following sections.

Symmetric Encryption

Symmetric encryption involves the use of a common key such as the Digital Encryption Standard (DES) and the many types of crypto materials created by the National Security Agency (NSA) for classified information. To pass secure information, each party must have the same key. The main problems with symmetric keys are that trusted distribution and advanced coordination are required to ensure a common key for all parties. The mechanics of encryption itself are relatively straightforward. The first party who wishes to send a secured message develops the plaintext message on a trusted machine; the encrypting device then uses the symmetric key to create a secure ciphertext, which is then transmitted; this text cannot be decrypted by anyone without the symmetric key. At the receiving end, the symmetric key is used to extract the cleartext from the ciphertext.

Asymmetric (Public Key) Encryption

The use of asymmetric or public key encryption (PKE) was developed by Rivest, Shamir, and Adleman at the Massachusetts Institute of Technology (MIT), hence referred to as RSA encryption. The advantage of PKE is that it allows for widespread and easy transaction security that involves less coordination. The use of PKE involves two different kinds of keys — public and private; each party has a private key "known" only to that party and a public key that is published for general knowledge of a "public" community. The mechanics of encryption are quite simple, broken into three different purposes for this method.

- **Confidentiality**. For a sender to send a message to a receiver using simple encryption (with *confidentiality* of delivery), the sender uses the public key of the receiver to encrypt the message; although anyone can intercept this text, only the receiver with the matching receiver private key can decrypt the ciphertext. The receiver's public and private keys are complementary — they encrypt and decrypt each other. See Exhibit 7-7-1.

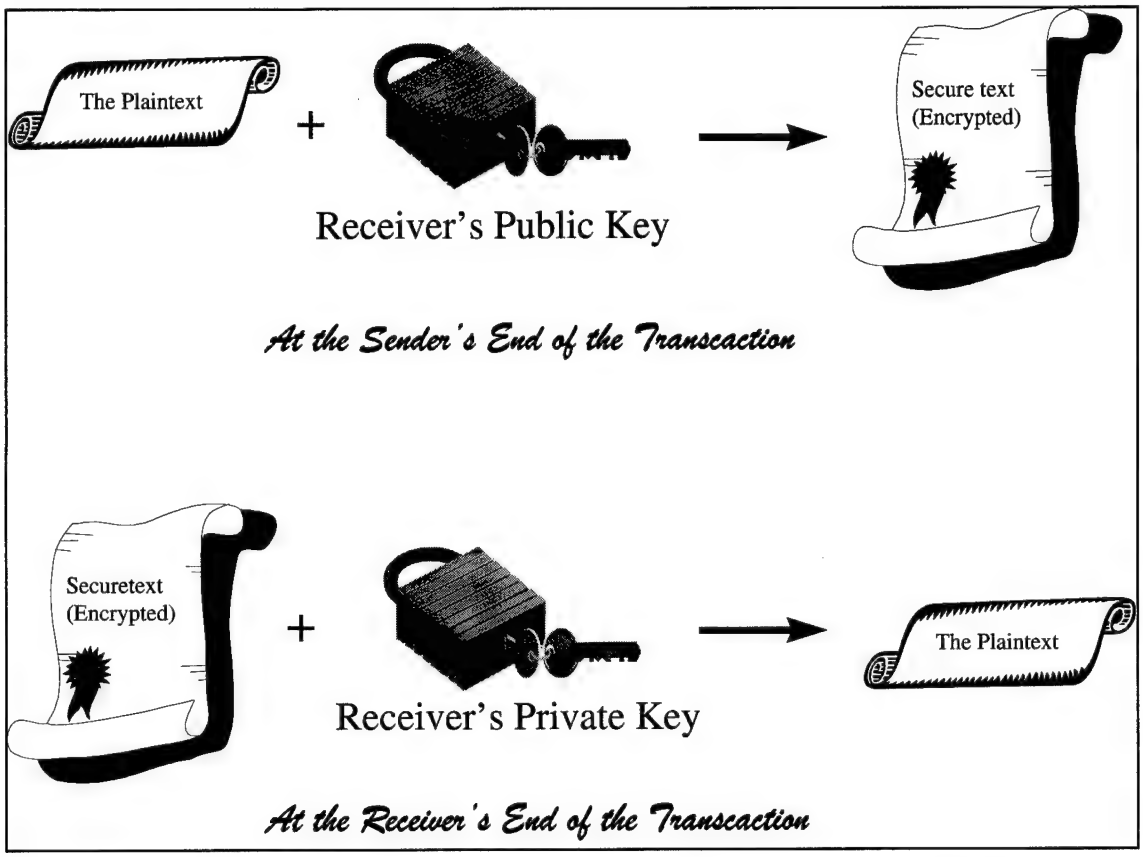


Exhibit 7-7-1. Process of Securing a Text Using Public Key Encryption

- **Authentication**. For ***authentication*** of a given message where the receiver wants to be sure that the sender has sent a given message, the sender encrypts the message with the sender's private key; the receiver then uses the sender's well-known public key to decrypt the ciphertext (encrypted). Although anyone can intercept this text and read it, the issue now is not confidentiality — in fact, this method of authentication often is used for a whole group to receive a message from an originator at the same time and verify the authenticity of the sender. The only problem with authentication is how to verify that the public key published is in fact that of the sender and not someone else. One method of validating public keys is the use of certification authorities, especially using the additional security of the Kerberos trusted distribution system. See Exhibit 7-7-2.

- **Authentication and Confidentiality**. For this difficult method of encryption, party "A" must provide assurance of identity and confidentiality as well. To do this, party "A" first encrypts the message using the party "A" private key (to establish authenticity); then that message is encrypted a second time using the party "B" public key (so that only party "B" can decrypt it — thus providing confidentiality). When party "B" receives the ciphertext message, it is decrypted using first the party "B" private key, and then decrypted again using the party "A" public key (so that "B"

knows it came from only party "A"). While this method is the most involved and it somewhat slow for lengthy messages, it is relatively secure and trustworthy.

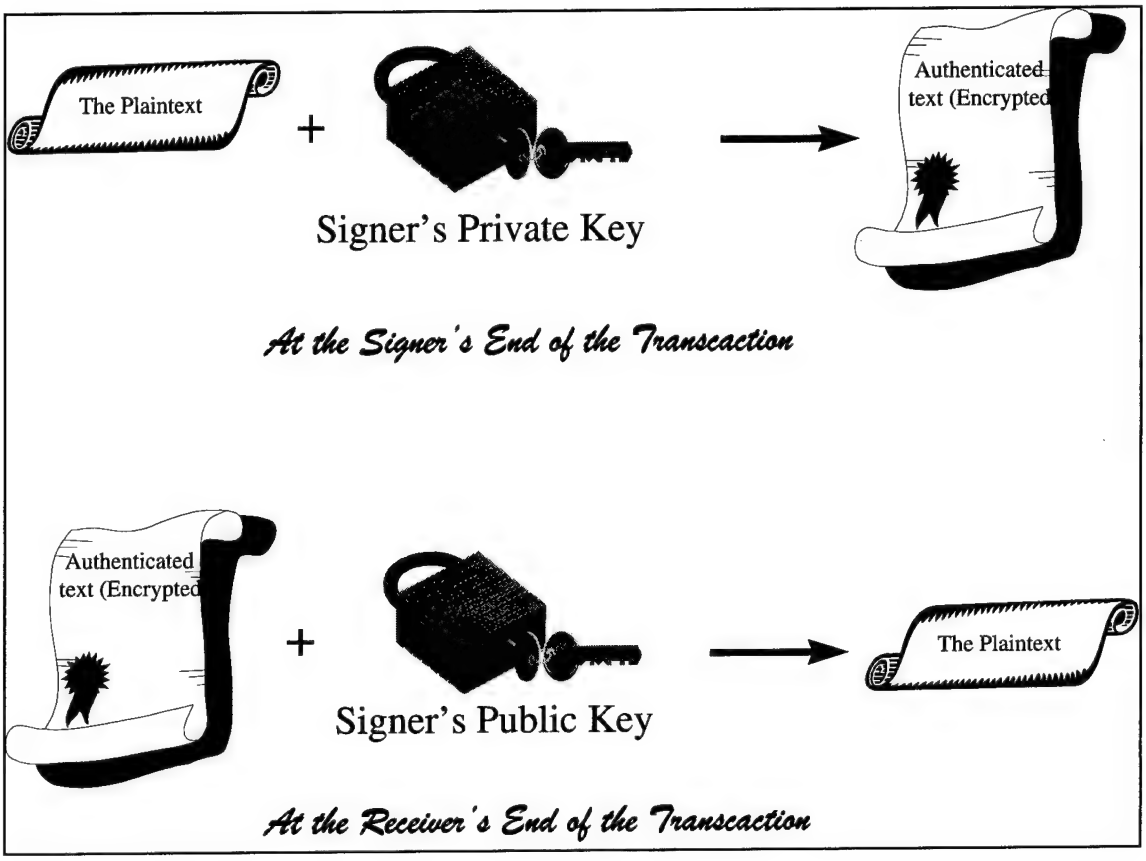


Exhibit 7-7-2. Process of Authenticating a Text Using Public Key Encryption

The actual technical method of doing this encryption involves the use of two extremely large prime numbers which are multiplied together to produce another huge number, as well as other mathematical complications involving modulo mathematics. When one has the product and one of the primes, it is relatively simple to recover the other prime through factoring. This process, however, is too complex for trial-and-error brute-force processing to work, short of using extremely high computers calculating for many years.

To achieve authentication for allowing access, the most common method is the use of a log-in string and use of a password or phrase. In addition to the use of passwords, there are several better hardware methods of achieving authentication. One is by use of a "smart card" that generates a one-time password in response to a challenge by the system at log-on or by swiping its magnetic stripe which checks the user who holds the card. A reader can check the pattern of the user's fingerprints or the unique eye structure through a retinal scan. These biometric devices are perhaps the most foolproof, but they are the most expensive.

7.7.2 Encryption Key Length

In a significant paper "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," Matt Blaze, Whitfield Diffie, Ronald L. Rivest, et al propose that 40-bit keys for symmetric encryption are no longer adequate to prevent brute-force attacks and even 56-bit keys are now effectively untrustworthy. They strongly recommend a minimum of 75 bits for today's keys and at least 90 bits to protect against advances in computer power in the next 20 years. The credibility of this article is strengthened by recognition that: Diffie was the creator of the Diffie-Hellman encryption scheme, one of the earliest and better encryption methods; and Rivest is one of the trio that pioneered research into public key encryption, lending his name as part of the RSA (Rivest, Shamir, Adleman) encryption. This latest report helps to frame current discussion on exporting technology for strong encryption (long keys). [272]

7.7.3 Key Escrow Policy/Events

A recent article in the *New York Times* by Steve Lohr details the findings of a distinguished panel of computer scientists reviewing the government's plans for key recovery. The article reports on the many issues arising from keeping the keys to unlock data-scrambling software to pursue criminals and terrorists on the Internet. The panel showed that the plan could actually increase security risks and raise the costs of online commerce. The researchers, in a study coordinated by the Center for Democracy and Technology, a nonprofit policy-research group in Washington, examined the technical challenges of the Government's Internet security proposal. The plan would permit U.S. computer companies to export powerful encryption software, but only if they established a system that would enable the keys to the code to be obtained by law-enforcement officials with a court warrant. The plan calls for these software "keys" — lengthy numeric codes — to be held not by a Federal agency, but by third-party organizations. To get the keys, law-enforcement officials or intelligence agencies would have to obtain legal authorization.

The plan to use third-party key holders was advanced last fall by the Clinton administration. It was made in response to concerns by civil liberties groups, including the Center for Democracy, that warned that letting a Federal agency hold the keys would make it too easy for Government to monitor the communications of private citizens. Further, the plan responded to complaints by software companies that it would hurt sales.

The 11 computer scientists — experts in the use of software that encrypts data — concluded that the Government's so-called key escrow plan, however well intentioned, would introduce its own set of risks and costs.

The administration's plan faces political opposition domestically and skepticism by some foreign governments. The House Judiciary Committee unanimously passed a bill to relax export controls on data-scrambling software and permit companies and individuals to use any encryption programs they choose.

---

[272] Matt Blaze et al, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," A Report by an Ad Hoc Group of Cryptographers and Computer Scientists (January 1996). On Internet at ftp://ftp.research.att.com/dist/mab/keylength.txt (in ASCII).

Germany said it would not do anything to regulate data-scrambling software for at least two years, waiting to see how Internet markets developed.

Lotus announced that its Lotus Notes product would include an escrowed key permitting the U.S. Government to decrypt any encrypted information in the groupware product. Privacy advocates took a very dim view of this change as it would strengthen the Clinton Administration Key Escrow proposal.

Legislation has been introduced in both the House and the Senate to permit export of data encryption hardware and software if similar technology is available from foreign suppliers. The bills would allow U.S. citizens to use any encryption which they choose and prohibit mandatory escrow of the key by anyone for use by law enforcement officials. The legislation is only for domestic use and makes it a crime to use encryption to cover up or assist in committing another crime.

7.7.4 New Encryption Standards

Users who currently require adequate or strong encryption to ensure the security of their information have a number of public and symmetric key standards, mechanisms, and products from which to choose. With passing time and the increasing speeds of computer processing, many of the older tools are becoming more vulnerable to "brute force" breaking of the key. Several bodies are working to develop new and more robust encryption standards for protecting particular types of information and/or types of transactions.

MasterCard, VISA, and others, in conjunction with cryptology experts, have developed a new encryption standard, the Secure Encrypted Transaction (SET) to allow secure transmission of financial (especially credit card) transactions on the World Wide Web. The proponents for related transactions, such as ANSI X12.58 for security electronic commerce/electronic data interchange (EC/EDI), have advanced several alternative possibilities of encryption schemes.

The National Institute for Standards and Technology (NIST) is currently working on a possible replacement for the venerable Digital Encryption Standard (DES) that has been used reliably for a number of years for symmetric encryption. The replacement, which will supersede DES, has been designated as the Advanced Encryption Standard (AES). This encryption standard probably will include strong encryption keys of 128-bits or more to ensure a reasonably long life until computation speed ultimately makes it obsolete.

7.7.5 Key Distribution and Management

Whether an organization uses a symmetric or an asymmetric (public) key scheme, the biggest problem is how to distribute the key to the users. For symmetric key architectures, the normal method, long used by DoD, has been to distribute the keys from the National Security Agency (NSA) using Armed Forces couriers. This system is both cumbersome and expensive. For civilian agencies and organizations, this alternative is not practical — hence, the trend toward public key encryption explained earlier. One critical problem with PKE is how to be sure that

the other party's supposed public key really belongs to them. With a small closed circle of users, pretty good privacy (PGP), an earlier PKE method provided by Phil Zimmermann, assures reasonable, but not total, security due to its lack of certification of the public key. Numerous agencies are providing key certificates to guarantee the authenticity of the public keys of users. These providers include Government agencies, large networking services, large corporations, and the major browsers such as Netscape.

Another valid method for assuring the authenticity of the public key of a given user is through the use of Kerberos technology. Kerberos is a specialized method of trusted symmetric key technologies. A trusted certification authority is used, in effect, to pass a symmetric key from one user to another in encrypted form without exposing the key to the network.

None of these methods addresses the issue of escrow. Since the Kerberos trusted certification authority handles the key(s) passed back and forth between the parties to the given transaction, that agent could retain a copy of the session key to decrypt the ciphertext passed, if a law enforcement agency requested it. Hence, the thorny question — should that agent retain a copy of the key or should true privacy be assured — emerges to force society to examine the larger issue of true privacy and Governmental control raised earlier about the encryption technology of SKIPJACK.

7.8 GOVERNMENT ENCRYPTION INITIATIVES

To promote the growth of electronic commerce and robust, secure communications worldwide, the Federal Government has proposed several initiatives. These initiatives balance that growth with protection of the public safety and national security interests. Liberalizing export controls for commercial encryption products will improve this balance.

During the transition to a global key management infrastructure, stronger cryptographic products are needed to protect individual rights to privacy, intellectual property, and other valuable information. Under this international infrastructure, trusted private sector parties will hold spare keys to confidential data. The data would only be recoverable by the key owner or by law enforcement acting under proper authority. A parallel is the master keys held by registered and bonded master locksmiths.

During the next 2 years, 56-bit cryptographic products will be exported. Before export, the Commerce Department reviews the exporter's commitment to develop key recovery features and support to the international infrastructure. The Administration is developing a formal mechanism that will enable industry, users, state, and local law enforcement, and other private sector representatives to predict the future of key recovery. This mechanism will include evaluating the developing global key recovery architecture, advising on technical confidence issues pertaining to access and release of keys, and addressing interoperability/standards issues. [273]

[273] Office of the Vice President news Release, 1 October 1996.

Another Government encryption initiative, the Clipper Clip, encompasses a new and technically superior encryption technology known as SKIPJACK. The Clinton Administration has proposed to make the new technology freely available for anyone in commerce, industry, or academia who wishes to use it. It serves as a free replacement for the aging Digital Encryption System (DES). Because of the claimed breaking of the DES algorithm, the new key is being used heavily. The one proviso that has numerous skeptics is that the Government would retain the master key. This retention would enable any enciphered text to be recovered by Government agents. The Administration is negotiating many possible alternate escrow agents and legal mechanisms to ensure trust by a large community. Many people are, however, still reluctant or unwilling to commit their secrets to the Government.

7.9 OPEN SYSTEMS/STANDARDS

In the past, many Defense communications and computer systems were proprietary and not well known outside their small, enclave-type communities. This factor had both advantages and disadvantages. On the one hand, few outsiders could break in easily since DoD architectures were closed, virtually unknown, and constructed quite differently from outside networks and systems; on the other hand, repairs and spares were more expensive and harder to obtain since the components were not common commercial off-the-shelf (COTS) items. In today's Defense networks and systems, the normal way of doing business, even mandated for interoperability reasons, is to use open systems with commercial standards (such as those published by the American National Standards Institute, the Institute for Electrical and Electronic Engineers, and the International Organization for Standardization). These systems and standards further the ready employment of COTS parts, architectures, and methods. Not only does this approach make it easier to get spares, but it also makes it easier for outsiders to intrude.

While there is no easy way to remedy the problems caused by COTS standards and methodologies, greater awareness of the hazards and an enhanced emphasis on increased security will greatly counter the downside of the COTS cost-benefit tradeoff. Some examples of the approaches recommended in numerous security communities include greater use of security layers, such as:

- Use *infrastructure design* principles to complement system and network design principles.
- Develop a thorough and reasoned security policy for Defense systems. Ensure adequate security staffing to implement and enforce security policy and procedures.
- Vigorously investigate and prosecute system and network intrusions. Visibly enforce all security policies.
- Segregate communications and automated information system networks through routers, controlled gateways, selected encryption. Use the best commercial security technology, especially state-of-the-art firewalls properly configured and maintained, to control the flow of information.

- Consider the need for data integrity checks, evolving protocols such as Kerberos and other certificate escrow means, new key types and greater key lengths to respond to technology changes.
- Use existing technologies to monitor systems and networks and detect intrusions. Include COTS *and* GOTS audit data reduction and analysis capabilities and intrusion detection capabilities.
- Consider appropriate methods of assuring integrity of control and authentication of users. This can be through security policy, written protocols, call-backs, and public-key authentication means.
- Build upon the strengths afforded by open systems by using cost-effective standardized security mechanisms: public key encryption (PKE) methods for access control, authentication, and digital signature to ensure the confidentiality of sensitive information. Although encryption is never a complete solution for security requirements, it should be used as needed.

7.10 INTERNET SECURITY AND VIRTUAL PRIVATE NETWORKS (VPN)

Standards and interoperability issues still stand in the way, but virtual private networks (VPN) are coming quickly. While many companies and Government agencies have set up private, encrypted networks using either dial-up or leased circuits, the expense of these is quite high. As organizations look to using the Internet to reduce their costs and enhance their business options, the question of the security of transactions, especially financial ones, arises. Numerous organizations are now looking to the creation of virtual private networks, a technology that allows a private network to be set up and encrypted *on the Internet.* Some of the various tools for setting up a VPN use the techniques of encryption along with tunneling, which involves encapsulating other protocols, such as IPX within the Internet protocol (IP).

One of the major problems in this new and evolving technology is that the standards have not been set to make it easy for two or more organizations to set up a VPN. For the encryption piece, many different security types and variants are available (RSA, PGP, DES, etc.) for the parties. For the tunneling process or encapsulation, two main protocols exist today: PPTP, used by Microsoft in its NT servers; and L2F, used by Cisco in its routers. A compromise standard that blends the two, L2TP, is in the draft phase at the Internet Engineering Task Force (IETF). Resolution of these standards' incompatibilities is the one major challenge to building VPNs; the other, perhaps, is to define what exactly is a VPN — quite a few technologies are grouped into the name, and there is a lack of agreement on its very nature and components.

7.11 SECURITY CONSIDERATIONS OF MOBILE CODE

In 1995, Sun Micro Systems announced the development of the Java language. What is especially new about it is that it can be used to program both applications and "applets." Applications are the normal programs that most people think of when they hear the term "programming language." Applications are source code programs compiled into running, executable code; the best known Java application is the "plug-in" for all browsers that interpret

Java applets. Applets are special programs written and compiled like Java applications, but they are included as attachments to regular Web pages written in hyper-text markup language (HTML). In fact, there is an HTML tag, "APP," which tells the Web browser (client program) to bring in and run (interpret) the Java byte-code program it requests from the server.

Java applet programs can be used to perform a number of exciting new applications, especially adding animation to "flat" Web pages that have only text, graphics, and other static displays. With the very visible activity of moving figures, "ticker-tape" banners, and response-soliciting behavior of Java applets, the interactive character of the next generation of tools has added a new dimension to the Internet. Java's new tools can help to eliminate the need for many helper applications now required to insert special features beyond text, into Web pages. Another helpful aspect in the Java development is that it is now well on its way to becoming an open industry standard. The possibilities that Java offers Internet and Intranet users are limited only by the creative imaginations of Web designers and programmers.

Java is not the only executable code addition to the Internet, and especially the World Wide Web. Microsoft is developing its own family of interactive tools known as ActiveX. The ActiveX family interacts very neatly with Visual Basic, the Visual C++ compiler (with its Object-Oriented development environment and its varied code libraries), Visual J++, and several other Web-oriented scripting languages. The ActiveX family provides many features similar or complementary to Java. It also meshes quite seamlessly with the Internet Explorer, the Microsoft Web browser which is competing with Netscape's Navigator. Due to the demands of the marketplace and the time-lead enjoyed by Sun's Java, the two families are largely compatible.

As an evolving open industry standard, ActiveX controls, formerly known as Object Linking and Embedding, are built on the Component Object Model. The ActiveX technologies enable developers to integrate reusable software components and use any language and platform to build Web, LAN, and PC-based applications. These object technologies adhere to the Internet standards and include client/server capabilities, tools, and applications.

The potential problem with Java and ActiveX controls is that, like HTML or regular text Web-pages, their code is downloaded to the user's computer and executed without any needed intervention. Since they have the power of any computer program, misguided programmers now have new methods that threaten security and privacy for users. A vindictive programmer who wants to threaten users of a particular community can insert code into an applet to delete data — all at once or selectively — or just modify it. Even as patches are developed, clever programmers work to circumvent them. The threat to the Defense, banking, insurance, financial services, infrastructure, and other communities is all too obvious. An important question is whether the problems can be fixed permanently or whether the (Java) interpreters should just be turned off in all corporate and Defense browsers.

Some utility designers, and especially browser designers, are creating modifications to verify authenticated code and also to allow users to filter out all applets of unknown sources or which contain certain code sequences known to be hostile. The continuing problem of identifying hostile sources, hostile code (such as viruses, logic and time bombs, and Trojan horses that can

be embedded into Java source code), and new ways to elude protections is daunting. In the meantime, many advocates of the philosophy of "better safe than sorry" advise caution by turning off the Java option in Internet browsers. Just as Java has had to deal with security holes, so too, the growing technology ActiveX must work to meet the challenges of security, whose demands are often counter to its aim of open transmission of information.. In short, both of these exciting new technologies, like most software developments, present many creative new possibilities, but users should not plan to use them on their computers without knowing the extensive risks and considering precautions.

7.12 SECURITY FLAWS AND FIXES

As noted above, most new software developments that bring benefits also come with unknown and unexplored flaws. Operating systems (OS) are especially prone to these problems. With the release of Windows 95 and the two iterations of Windows NT (3.51 and 4.0), at least several security holes have been noted. These problems also have followed the releases of new versions of the Apple Macintosh operating system, the new POSIX-compliant LINUX operating system for UNIX machines, and other high quality OS products. As windowed operating systems become increasingly complex and sophisticated software products, the chances of vendors exploring every possible flaw by tracing every possible path through the code decreases.

Fortunately, as hackers hit the weak spots and cause repairs to be made, as academics probe the software for holes and report them, and as the vendors themselves keep searching for holes that expose users' data to harm (and themselves to liability suits), software gradually has become more functional and safer. But safety demands that "patches" or "fixes" be installed promptly and correctly; this requires that the vendors widely publicize these needed modifications. Additionally, systems administrators and individual users must know how to install, optimize, customize, and adapt the modifications to the original software package. The bottom line is that any system is only as secure as the latest software fix that has been installed.

7.13 COOKIES

Another of the many features of Internet programming, whose original intent was to be of service but which has easily been turned into a security and privacy threat, is that of "cookies." These small text-insertions into the Web browser for Internet transactions were intended from the beginning to provide a service, speeding up the transaction, especially its initiation. For many transactions providing a hypertext link to another Web page, the person or institution who owns the server often wants to speed up the link process to make the service available to more users. One way of doing this is for the server to pass the browser client an identifying token which will provide the server information to avoid a new dialog the next time the user visits that site. The ID can include a password, a preferred display mode, and other helpful information.

One might wonder why the server does not maintain this information in its files. The obvious answer is that the number of visitors is almost endless and many visitors may access the site only once. So the solution is for the client to store all this information on the user's computer in a

special file, perhaps encrypted. Although this enables the server to help more users, one has only to think about this arrangement briefly to fathom the abuses that are possible.

First, in the cookie itself, malicious code can be hidden that can initiate any number of ill effects upon certain triggers — on particular key dates, Web site accesses, or conditions (such as disappearance of the employee from the payroll). Second, the information stored in the cookie can be used for purposes of spying or otherwise invading the privacy of the user. The obvious question is whether, for security purposes, one should ever accept any cookies. Technically, it is not too difficult to instruct most main commercial browsers, such as the Netscape Communicator or Microsoft Internet Explorer, not to accept any cookies. But it may make for longer and more tedious exchanges with sites one frequently visits. Certain sites furthermore may refuse services without the exchange of cookies, due to the fact that the absence of a cookie will lengthen all transactions in the future — cookies do streamline transactions and allow more accesses for other users. The bottom line for security is that acceptance of cookies from known sites is done with minimal risk, whereas acceptance from unknown sites is done at possibly large risk

7.14 FLOODING AND THE SYN-ATTACK

The intent of servers, as the name suggests, is to provide a service to the users who access the special purpose computer. Any authorized user can access the server and request the intended service, such as transferring files, executing certain programs, etc. The hazard of having a server open to all of the users of the Internet is that certain users may have a grudge, an ideological difference, or another reason to cause harm to the server, especially by denying its use to other users. Although this may seem like a momentary annoyance, it can have severe impact upon financial, Defense, medical, infrastructure, and many other types of servers that users rely upon in times of crisis or just ordinary circumstances. One of the more publicized incidents of these denial-of-service hacks has been by use of the SYN-flooding technique that takes advantage of a weakness of the TCP packet exchange protocol. Other flooding techniques continue to be devised by clever, but mischief-making, users. The most unfortunate aspect of these hacks is that cures to the problem are still not readily available.

7.15 SINGLE SIGN-IN LOGONS

One of the biggest problems encountered by many users is that of having to remember the many passwords and log-on routines required to access numerous different network services. The obvious solution for many users is to write down the different things that must be remembered, which violates good security practice. Another easy, but also undesirable, solution is to have the computer store all these passwords and access log-on routines. Since it could allow unauthorized persons to use these services, this storage solution can be somewhat dangerous and possibly counter to good security policies. One solution that has been worked out by vendors is to create an encrypted secured-storage (encrypted) method of capturing and preserving a single log-on service. This approach now makes it unnecessary for the user to see more than the initial log-on screen — the multiple access routines thus become transparent to the user. Advantages and disadvantages of this solution have yet to be weighed in long-term practice.

7.16 FIREWALLS

Like the VPN technology mentioned previously, the term "firewall" is one which does not have a commonly-understood meaning. In fact, it denotes a wide range of technologies, not a single one as the name would lead one to believe. The term "firewall" refers to any structure that protects a user from an outside threat, such as a forest fire. In the world of information security and assurance, a "firewall" refers to various technical structures, both hardware and software, that can be used to protect an internal network from any intruder. There are two main classes of firewalls: application and packet filters. An application filter determines which applications a given authenticated user may access. A packet filter examines the structure of every packet that is sent to it to determine the source, the addresses to which it may be sent, and other authorization issues. Firewalls have become more and more sophisticated as the threat has become smarter.

While managers may attain some measure of comfort by deploying a firewall in their networks to provide increased protection, there is a cost. Firewalls demand more knowledgeable systems administrators; and some of the larger networks with the most technically sophisticated firewalls demand *full-time* administration. The most complex firewall systems (and this name is quite appropriate) involve use of bastion hosts, subnets, large and detailed router tables, and other technologies to help secure the network from undesired outside accesses. One of the most important security requirements with today's improved firewalls is constant administration of all the features by people who know how to use their capabilities.

7.17 THE YEAR 2000 (Y2K) PROBLEM

The National Computer Security Association (NCSA) reported that the addition of only *one* second to the year in the beginning of 1996 caused significant problems with software controlling the broadcast of Coordinated Universal Time from NIST. This tiny addition to clocks at the start of the year caused the software to advance the date by a whole day! Another example illustrates the problems that reside in date-based software — a correspondent in the "NCSA RISKS" reported messages received on February 29, 1996 were dated variously by different E-mail systems as 29 Feb 96, 28 Feb 96, 1 May 131, 10 Jan 1936, 1 Jan 70, and 29 Dec 95. [274] This type of problem appears insignificant when compared with the major problems expected with the larger change into the year 2000.

With millions of lines of code locked into two-digit year fields like "97," the arrival of the year 2000 ("00") will present problems. The largest problem is that 2000 will be interpreted as 1900 and transactions involving arithmetic operations, such as subtracting dates, will result in erroneous results (such as a negative number, which will be rejected). Thus, many programs written in earlier patterns will fail to process transactions as intended. In fact, several industries, notably financial services, already are starting to see the problems occasioned by the misinterpreted dates. Some banks with loan transaction programs written in older-style COBOL are finding that an entry for a loan to start in July 97 (1997) and ending in July 02 is seen as ending in July 1902 (an impossibility that causes the program to terminate without making the

[274] Reported in M.E. Kabay, *The INFOSEC Year in Review: 1996* (National Computer Security Association: 1997). On NCSA Internet site at http://www.ncsa.com/library/isecyir.html

transaction). Many institutions are in the process of changing the programs that depend upon date-entry transactions, but the number of lines of code to be checked and changed is staggering. As many are discovering, the problem is relatively simple to fix, but that the size of the problem is huge. The problem is compounded by several complications: the number of computer programmers who know the older programming languages is continually decreasing; the number of programmers who want to learn these older technologies to solve this huge problem and then become quickly obsolete, is far short of the requirement; and finally, the time to recognize, accept, and work on a fix is decreasing, unrelentingly.

Although this may not seem to be a security problem, it could likely affect the security of the entire Information World (the G-7 nations and many others have staked their way of life on the use of information). A significant consequence of this problem is the large budgetary outlay that will have to be committed over the next 3 years to fix *most* of the problem (some estimates run into the hundreds of billions of dollars worldwide). Perhaps the worst aspect of this problem is that there cannot be any extension granted to solve it — 2000 is barely 2 years from now. One last aspect with security implications is how will Defense, Government agencies (Federal and state), and other key institutions react and cope as many major computer and other systems fail over the next 5 years.

7.18 NETWORK SECURITY

Perhaps the most pressing venue for development of security technologies (and strategies, in general) is the network. The network must be viewed from all perspectives — the Local Area Network, the Metropolitan Area Network, the Wide Area Network, the Global Area Network, the Internet, the Intranet, and the Extranet. Simply viewing the above network terms and trying to define their boundaries, media, and technologies illustrates the speed of technological change. Approaching network security demands the unified and overall vision of strategy, doctrine, policy, and operational practices discussed in previous sections of this report. The technology, however, cannot be readily unified since the network technology variants are already numerous: network operating systems (NOS), topologies, architectures, etc. The vendors of different NOSs, such as Windows NT and of the many variants of UNIX/POSIX, and VINES, incorporate specialized security mechanisms into their products and struggle to keep them one step ahead of the "wily hacker." The Ethernet, Token Rings, wireless, and varied copper and fiber topologies all present new challenges to vendors and systems administrators. Finally, the shifting orientation from the mainframe to the various multi-layer client-server architectures demand continuously updated security solutions.

With the explosive growth of the Internet and its extensions into the Enterprise — through Intranets and Extranets — the security challenges require manifold responses. Previous sections have addressed the many areas of technological growth that are advancing the security discipline from a technology perspective — encryption, virtual private networks/ protocol tunneling, and firewalls, among others. Additional new or developing technologies that promise further relief include: better user identification/authentication through easier, cheaper, and more effective biometrics which are spreading more into commercial practice; and Internet security standards

and protocols (such as SSL, IPSEC, SET, IPv6, ISAKMP) which are continually being adopted and adapted into new products.

SUMMARY

- DARPA, SEI, DISA, and the INFOSEC Research Council are pursuing powerful avenues of research, development, procedures, and tools to aid in the growth of information security and information assurance.
- Intrusion detection tools are helping to deal with the threat of "crackers" — amateur, professional, and state-sponsored terrorists.
- Encryption is improving and becoming an even more powerful tool to safeguard data, but it is not a "silver bullet."
- The utility and widespread use of the Government-developed Clipper chip is very much in doubt.
- Open systems, standards, and architectural methods open up computer systems to greater exposures and threats.
- Virtual private networks will offer numerous advantages in security, privacy, and cost-reduction. But standards and interoperability are still problems to be resolved.
- Java, ActiveX, and other download-able code present a new dimension of interactive tools for the benefit of Internet users.
- Many sophisticated programs, especially operating systems, have security flaws that expose information systems to various risks.
- "Cookies" are small text files passed to a browser client that enable a Web-server to recognize the user and serve information needs better.
- Flooding and the SYN-Attack present a severe denial-of-service threat to all information providers and other computers.
- Single sign-in logons are becoming available in the commercial market.
- Firewalls are not a single security technology, but rather a strategy employing numerous methods of hardware and software that require more highly-skilled systems administrators to set up and constantly update them.
- The Year 2000 may bring a new problem that is different and perhaps more difficult to overcome than many other classical security requirements.
- Biometrics and new security products offer continuing network and Internet security capabilities.

This page intentionally left blank.

APPENDIX A

REFERENCES

BOOKS, MONOGRAPHS, BROCHURES, AND PAMPHLETS

Alberts, David. *Defensive Information Warfare*. Washington, DC: Institute for National Strategic Studies, National Defense University, 1996.

Elias, Stephen and Susan Levinkind. *Legal Research: How to Find and Understand the Law*. Berkeley, CA: Nolo Press, 1995, pp. 6/40-41.

Howard, John D. *An Analysis of Security Incidents on the Internet 1989-1995.* Dissertation, Carnegie Mellon University, 7 April 1997. Available on Info-sec.com Internet site at http://www.info-sec.com/Internet/howard/Start.html.

Kabay, M.E. *The INFOSEC Year in Review: 1996*. National Computer Security Association, 1997. On NCSA Internet site at http://www.ncsa.com/library/isecyir.html

Rose, Lance. *First Amendment Protection for Networks and On-Line Systems, The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*. Computer Law Association, 1996. On Computer Law Association Internet site at http://cla.org/RuhBook/chp10htm

ARTICLES, CHAPTERS, CONFERENCE PAPERS, PRESENTATIONS, LECTURES

"Export Granted for 56-Bit Encryption," *InfoSecurity News* 8 (May 1997) 3:14.

"Joint DoD Exercise Reveals Military IW Vulnerabilities," *Defense Information and Electronic Report* 2 (11 July 1997) 28:1.

"US uses first court-ordered wiretap on computer network," *Nando.net* (29 March 1996). On Nando.net Internet site at http://www2.nando.net/newsroom/ntn/biz/032996/biz9_7625.html

Bank for International Settlements. "Security of Electronic Money, a Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries," August 1996. On Bank for International Settlements Internet site at http://www.bis.org/publ/index.htm

Barshefsky, Charlene. Statement by the Honourable Charlene Barshefsky, Acting United States Trade Representative. World Trade Organization Ministerial Conference, December 1996.

Barshefsky, Charlene. Statement of Ambassador Charlene Barshefsky. "Basic Telecom Negotiations," 15 February 1997. Office of the US Trade Representative Internet site at http://www.ustr.gov/agreements/telcom/barshefsy.html

Biegel, Stuart. "Reflecting Back On 1996: The Year That Cyberspace Law Came Of Age," *L.A. Daily Journal* (January 23, 1997). Reprinted by the UCLA Online Institute for Cyberspace Law and Policy, On Internet at http://www.gse.ucla.edu/iclp/jan97.html

Blaze, Matt et al. "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security." A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996. On Internet at ftp://ftp.research.att.com/dist/mab/keylength.txt (in ASCII).

Brown, Raysman, Millstein, Felder & Steiner LLP. "California Federal Court Again Holds Encryption Software Protected by First Amendment." On Brown Raysman Millstein Felder & Steiner LLP Internet site at http://www.brownraysman.com/docket/bernstn.htm

Chang, Keith. "G7 Information Society Pilot Projects: An Overview and the Current Status." Presented at the EITC '96, Brussels, 25-27 November 1996.

Chong, Rachelle B. Statement "Interesting Times at the FCC." Remarks of FCC Commissioner at University of California Berkeley, 27 June 1997. On FCC Internet site at http://www.fcc.gov/speeches/chong/sprbc707.html

Chong, Rachelle B. Statement "Amendment of the Commission's Regulatory Policies to Allow Non-US-Licensed Space to Provide Domestic and International Satellite Service in the United States (DISCO 96-111; CC. Doc. No. 93-23; File No. ISP-92-007)," 17 July 1997. On FCC Internet site at http://www.fcc.gov/Daily_Releases/Daily_Business/1997/db970717/discorc.txt

Dicther, Mark S. and Michael S. Burkhardt. "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age." Presented at The American Employment Law Council, Fourth Annual Conference, Asheville, North Carolina, October 2-5, 1996.

Fontana, John. "Sun Crypto Skirts Feds," *Communications Week* (19 May 1997).

Gaudette, Philip and Eduardo Talero. "Harnessing Information for Development: A Proposal for a World Bank Group Strategy," The World Bank, 1 April 1996. On the World Bank Internet site at http://www.worldbank.org/html/fpd/harnessing/hid2.html

Hernandez, Dennis F. and David May. "Personal Jurisdiction and the Net: Does Your Website Subject You to the Laws of Every State in the Union?", *Los Angeles Daily Journal* (15 July 1996). Reprinted by the UCLA Online Institute for Cyberspace Law and Policy. On Internet at http://www.gse.ucla.edu/iclp/dhdm.html

Hill, Lisa Marilyn. "Electronic Mail in the Workplace." *MTTLR News* (April 1997). On University of Michigan Internet site at http://www.law.umich.edu/mttlr/news/index.html#stories

Hundt, Reed E. "Spectrum Policy and Auctions: What's Right, What's Left." Remarks to Citizens for a Sound Economy, 18 June 1997. On FCC Internet site at http://www.FCC.gov/Speeches/Hundt/spreh734.htm

Kelley, Patrick W. "The Economic Espionage Act of 1996." *The Law Enforcement Bulletin.* US Department of Justice, Federal Bureau of Investigation (1 July 1997). FBI Law Enforcement Bulletin Internet site http://www.fbi.gov/leb/leb.htm

Network Reliability and Interoperability Council. Minutes of 20 May 1997 meeting. FCC Internet site http//www.fcc.gov/oet/info/orgs/nric/meetings/m970520.html

Pooley, James H. S. and David M. Shaw. *The Emerging Law of Computer Networks, Finding Out What's There: Technical and Legal Aspects of Discovery*, 1997. Fish and Richardson Internet site, http://www.fr.com/working publis

Reinsch, William A. *Administration Encryption Policy*. Testimony before the Subcommittee on International Economic Policy and Trade House Committee on International Relations 8 May 1997. United States Department of Commerce, Bureau of Export Administration Internet site, http://www.bxa.doc.gov/warcong7.htm

Smith, Robert Ellis. "Searches and Surveillance in the Workplace" *Privacy Journal* (undated): 1-2.

The University of California Los Angeles (UCLA) Online Institute for Cyberspace Law and Policy, *Personal Jurisdiction: An Emerging Controversy Heats Up,* 1 October 1996. On UCLA's Internet site at http://www. gse.ucla.edu/iclp/cyberjurisd.html

GOVERNMENT / PUBLIC DOCUMENTS, STATUTES, CASES

Commission on the Roles and Capabilities of the United States Intelligence Community. *Preparing for the 21st Century: An Appraisal of US Intelligence,* 1 March 1996.

Congress, House of Representatives, Committee on Science, Press Release on H.R. 1903, the *Computer Security Enhancement Act of 1997*, by F. James Sensenbrenner, Jr., Chairman, 17 June 1997. On United States House of Representatives Committee on Science Internet site at http://www.house.gov/science/welcome.htm

Critical Infrastructure Working Group (CIWG). *Report of the Critical Infrastructure Working Group: Options for Protecting Critical National Infrastructures*, 6 February 1996.

Daniel J. Bernstein v US Department of State et al. can be found on Internet at http://www.eff.org/pub/Leagal/Cases/Bernstein_v_DoS/Legal/961206.decision

Defense Information Systems Agency, *The Technical Architecture Framework for Information Management,*(version 3.0). Available on the DISA Internet site at http://www-library.itsi.disa.mil/tafim/tafim3.0/pages/tafim.htm

Department of the Air Force. *The 1997 Air Force Long Range Plan: Summary.* Available on Air Force Internet site at http://www.xp.hq.af.mil/xpx/7frame.htm

Department of the Air Force. USAF Fact Sheet 95-10 "Air Intelligence Agency." On USAF website at http://www.af.mil/news/factsheets/Air_Intelligence_Agency.html .

Department of the Air Force, *Cornerstones of Information Warfare* on Air Force Internet site at http://www.af.mil/lib/corner.html

Department of the Air Force. *Global Engagement: A Vision for the 21st Century Air Force.* On Internet site maintained by Headquarters, US Air Force at http://www.xp.hq.af.mil/xpx/21/nuvis.htm

Department of the Air Force. Air Force Policy Directive (AFPD) 33-2 *Information Protection*, 1 December 1996. Available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

Department of the Air Force, Air Force Policy Directive (AFPD) 31-4 *Information Security*, 1 August 1997. Available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

Department of the Air Force, Air Force Doctrine Document 50 *Intelligence*, 1 May 1996. Available on Federation of American Scientists Internet site at http://vwww.clark.net/fas/irp/doddir/usaf/50.htm

Department of the Air Force, Office of the Staff Judge Advocate, Air Force Office of Special Investigations. *Legal Guidance*, by Elizabeth A. Banker, Robert E. Giovagnoni, Alexander R. Smith, and John T. Soma, 1996.

Department of the Air Force, Air Force Instruction (AFI) 10-1101 *Operations Security*, 1 May 1997. available on Air Force Internet site at http://afpubs.hq.af.mil/elec-products/pubs-pages/

Department of the Army, *Army Vision 2010*, undated. Available on Internet at http://www.army.mil/2010/

Department of the Army, Field Manual 100-6 *Information Operations*, 27 August 1996. Available from US Army Training and Doctrine Command Training and Doctrine Literature home page Internet site at http://www.atsc-army.org/atdls.html.

Department of Commerce, "Report on International Organizations," by James A. Johnson, March 1997. On US Department of Commerce NIST Internet site, nii.nist.gov/pubs/intl_org.html

Department of Commerce, Information Infrastructure Task Force, "The Global Information Infrastructure: Agenda for Cooperation," February 1995.

Department of Commerce (DOC), National Institute of Standards and Technology (NIST). Special Publication (SP) 500-167 *Information Management Directions: The Integration Challenge*, September 1989.

Department of Commerce (DOC), National Institute of Standards and Technology (NIST). Special Publication (SP) 800-11 *The Impact Of The FCC's Open Network Architecture On NS/EP Telecommunications Security,* February 1995. On NIST Internet site at http://osi.ncsl.nist.gov/snad-staff/olsen/pubs/titleona/titleona.html

DoD. *DoD Organization and Functions Guidebook*, September 1996. Available on DoD Internet site at http://www.defenselink.mil/pubs/ofg.html

DoD. *Report of the Quadrennial Defense Review*, May 1997.

DoD, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASDC3I). *Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense*, 28 March 1997.

DoD, Department of Defense Directive (DoDD) S-3600.1 *Information Operations (IO) (U),* 9 December 1996.

DoD, DoDD TS3600.1, *Information Warfare* (U), 21 December 1992.

DoD, DoDD 5100.1 *Functions of the Department of Defense and Its Major Components,* 25 September 1987.

DoD, DoDD 5160.54 *Critical Asset Assurance Program*, Draft, 6 June 1997.

DoD, DoD Instruction *DoD IT Security Certification and Accreditation Process (DITSCAP)*, Draft, 12 May 97 On Internet at DISA site http://mattche.iiie.disa.mil/ditscap/DODI_total.html

DoD, CJCS. *Joint Vision 2010*, undated.

DoD, CJCS. CJCSI 3210.01 (SECRET) *Joint Information Warfare Policy* (U), 2 January 1996.

DoD, CJCS. CJCSI 6510.01A *Defensive Information Warfare Implementation*, 31 May 1996.

DoD, CJCS. CJCSI 6510.01B *Defensive Information Operations,* Draft, 30 June 1997.

DoD, Director of Defense Research and Engineering. *Defense Technology Area Plan,* April 1996.

DoD, DISA. *Joint Information Assurance Operations Working Group (JIWG).* Briefing by Major Dexter R. Handy, 31 July 1997.

DoD, The Joint Staff. *Concept for Future Joint Operations*, undated. Available from Joint Staff site on Internet at http://www.dtic.dia.mil/doctrine/jv2010/concept.html

DoD, The Joint Staff. Joint Publication 1-02 *DoD Dictionary*. On Joint Electronic Library Internet site at http://www.dtic.mil/doctrine/jel/doddict/

DoD, The Joint Staff. Brochure *Information Warfare: A Strategy for Peace... The Decisive Edge in War*, 1996.

DoD, The Joint Staff. Joint Publication 2-0 *Joint Doctrine for Intelligence Support to Operations*, 5 May 1995.

DoD, The Joint Staff, Information Assurance Division (J6K). *The State of Information Risk Management Methodology*. By Science Applications International Corporation (SAIC), 8 August 1997.

DoD, The Joint Staff. Joint Publication 3-13 *Joint Doctrine for Information Operations,* Second Draft, 2 July 1997.

DoD. The Joint Staff. Publication 3-13.1 *Joint Doctrine for Command and Control Warfare (C2W)*, 7 February 1996.

DoD, OUSD(P), Critical Infrastructure Protection Working Group (CIPWG). *Options for Protecting the Critical National Infrastructures*, 6 February 1996.

DoD, Undersecretary of Defense for Acquisition and Technology (USD(A&T)). Memorandum for the Chairman, Defense Science Board , 4 October 1995.

DoD, Under Secretary of Defense for Acquisition and Technology. *Joint Warfighting Science and Technology Plan* , January 1996.

DoD, Office of the Under Secretary of Defense for Acquisition and Technology Defense Science Board (DSB). *Report of the Defense Science Board Task Force on Information Warfare - Defense*, November 1996.

DoD, Commander in Chief US Atlantic Command. Memorandum for: IW Wargame Participants: "Legal Aspects of Peacetime Information Warfare Command and Control," 29 January 1996.

DoD, United States Strategic Command. *Information Operations Threat Conditions Definitions and Measures Proposal.* 15 May 1997.

Dept. of Energy, Lawrence Livermore National Laboratory. *National INFOSEC Technical Baseline: Firewalls*, April 1997. On Internet at http://doe-is.llnl.gov/nitb/nitb.html

Dept. of Energy, Sandia National Laboratories. *US Infrastructure Assurance Prosperity Game™ Summary*. Briefing to NSTAC IES, 22 May 1997.

DOJ, Computer Crime and Intellectual Property Section. *Legislative Analysis: The National Information Infrastructure Protection Act of 1996*, undated.

DOJ, Federal Bureau of Investigation (FBI). Fact Sheet "CITAC Mission." Provided by FBI on 10 July 1997.

DOJ, Federal Bureau of Investigation. "Implementation of Section 104 of the Communications Assistance for Law Enforcement Act: Second Notice and request for comment." *Federal Register* 62 (14 January 1997) 9.

DOJ, Federal Bureau of Investigation. Statement before the Senate Judiciary Committee Hearing on Encryption, by Louis J. Freeh, Washington, DC, 9 July 1997.

Department of the Navy. Naval Doctrine Publication 2 *Naval Intelligence*, undated. Available on Federation of American Scientists Internet site at http://vwww.clark.net/fas/irp/doddir/navy/ndp2.htm

Department of the Navy. Secretary of the Navy Instruction SECNAVINST 3430.27 *US Naval Computer Network Incident Response, Draft.* Copy provided by Dept. of Navy staff.

Executive Office of the President. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Available on National Counterintelligence Center (NACIC) Internet site at http://www.nacic.gov/fy96rpt.htm

Executive Office of the President, OMB. "Computer Difficulties Due to the Year 2000 - Progress Reports," 7 May 1997.

Executive Office of the President, OMB. "Getting Federal Computers Ready for 2000," 15 May 1997. CIO Council Internet site, http://www.cio.fed.gov/yr2krev.htm

Executive Office of the President, OMB. Memorandum M-97-16 *Information Technology Architectures*, 18 June 1997.

Executive Office of the President, OMB. Transmittal Memorandum 69 *Preparation and Submission of Strategic Plans and Annual performance Plans*, 23 May 1997.

Executive Office of the President, OMB. Circular Number A-130 *Revised Management of Federal Information Resources*, 8 February 1996.

FCC. Press Release. "Regarding Judicial Ruling on Interconnection Rules." By Susan Ness, 18 July 1997. FCC Internet site at http://www.fcxc.gov/speeches/ness

FCC. Commission Action "Commission Initiates Proceeding to Review Rules and Policies on Foreign Participation in the US Telecommunications Market." 4 June 1997. FCC Internet site, http://www.fcc.gov/Daily_Releases/Daily_Business/1997/db970605/nrin7019.html

FCC, FCC 97-252 "Further Notice of Proposed Rulemaking, In the Matter of Amendment of the Commission's Regulatory Policies to Allow Non-US-Licensed Space Stations to Provide Domestic and International Satellite Service in the United States and Amendment of Section 25.131 of the Commission's Rules and Regulations to Eliminate the Licensing Requirement for Certain International Receive-Only Earth Stations and COMMUNICATIONS SATELLITE CORPORATION Request for Waiver of Section 25.131(j)(1) of the Commission's Rules As It Applies to Services Provided via the INTELSAT K Satellite," 18 July 1997.

GAO. Report to Congressional Committees GAO/NSIAD-97131 *Defense Communications: Federal Frequency Spectrum Sale Could Impair Military Operations*, June 1997.

GAO. GAO/AIMD-96-110 *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, September 1996.

Government Information Technology Services (GITS) Board. *Access America: Electronic Government - "Serving The Public On Its Terms"* - Chapter A15: "Integrate The Government Services Information Infrastructure" on Internet at http://www.gits.fed.gov/htm/gsii.htm

Government Printing Office. *Federal Register* 62 (June 23, 1997) 120. From the Federal Register Online via GPO Access at http://www.access.gpo.gov/su_docs/aces/aces140.html

Information Infrastructure Task Force (IITF) National Information Infrastructure (NII) Securities Issues Forum. *NII Security: The Federal Role*, 5 June 1995. On National Institutes of Health

Internet site at http://irma.od.nih.gov/security/niisec~1.html and National Security Institute site at http://nsi.org/Library/Compsec/nii.txt

ITU. "Buenos Aires Declaration on Global Telecommunication Development for the 21st Century," 1995.

National Imagery and Mapping Agency, *FACT SHEET*, from NIMA Internet site at http://www.nima.mil

National Communications System (Technology and Standards Division), Federal Standard 1037C (FS-1037C), *Telecommunications: Glossary of Telecommunications Terms.* Published by General Services Administration Information Technology Service, 7 August1996. Available for viewing at http://www.its.bldrdoc.gov/fs-1037.

National Computer Security Center (NCSC). *Glossary Of Computer Security Acronyms* (Aqua Book), 21 October 1988. Available on NIST Internet site at http://csrc.nist.gov/secpubs/rainbow/tg004.txt

National Security Telecommunications and Information Systems Security Committee (NSTISSC). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009 *National Information Systems Security Glossary*, January 1996.

Office of the Director of Central Intelligence (ODCI). "United States Intelligence Community." On United States Office of the Director of Central Intelligence Internet site at http://www.odci.gov/cia/other_links/wheel/index.html

The President, Executive Order 12139. *Exercise Of Certain Authority Respecting Electronic Surveillance,* 23 May 1979. Available on Federation of American Scientists Internet site at http://www.fas.org/irp/offdocs/eo12139.htm

The President, Executive Order 12333 *United States Intelligence Activities,* 4 December 1981. Available on Federation of American Scientists Internet site at http://www.fas.org/irp/offdocs/eo12333.htm

The President, Executive Order 12924 *Administration of Export Controls on Encryption Products*, 30 December 1996. White House Internet site, http://www.whitehouse.gov/

The President, Executive Order 12958 *Classified National Security Information*, 17 April 1995. White House Internet site, http://www.whitehouse.gov

The President, Executive Order 13010 *Critical Infrastructure Protection*, 15 July 1996.

The President, Executive Order 13011 *Federal Information Technology*, 17 July 1996.

The President, National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (superseded NSDD-1455), 5 July 1990

The President, Presidential Decision Directive (PDD) 29 *Security Policy Coordination*, 16 September 1994.

President's Commission on Critical Infrastructure Protection, *Overview Briefing*, June 1997. On the Commission Internet site at http://www.pccip.gov/info.html on 1 August 1997.

President's Commission on Critical Infrastructure Protection, *Hacker Primer*, 5 April 1997. (Note: some copies misprinted with date 5 April 1996).

President's National Security Telecommunications Advisory Committee, Information Assurance Task Force. *Electric Power Information Assurance Risk Assessment*, March 1997.

President's National Security Telecommunications Advisory Committee, Information Assurance Task Force. *Financial Services Risk Assessment Report*, June 1997.

President's National Security Telecommunications Advisory Committee, Information Protection Task Force, *Plan of Action*, 15 August 1996.

United Nations, *Model Treaty*. At United Nations Crime and Justice Information Network Internet site, http://www.ifs.univie.ac.at:80/~uncjin/unrule17.html

United States. *Telecommunications Act of 1996.* Pub. LA No. 104-104, 100 Stat. 56 (1996). Full text available of U.S. Federal Communications Commission (FCC) site on Internet at http://www.fcc.gov/telecom.html

US Code of Federal Regulations. *Export Administration Regulations (EAR),* 15 CFR Parts 730-774 (7 January 1997).

USMC, Marine Corps Doctrinal Publication (MCDP) 6 *Command and Control*, October 1996.

INTERNET SITES

Asia-Pacific Economic Cooperation (APEC) http://www.apecsec.org.sg/apecnewinfo.html

Chief Information Officers (CIO) Council http://www.cio.fed.gov

Cornell University School of Law gopher://gopher.law.cornell.edu:70/00/foreign/fletcher

Defense Advanced Projects Research Agency (DARPA) http://www.darpa.mil

Department of the Air Force, Air Force Information Warfare Center (AFIWC) http://www.aia.af.mil/aialink/homepages/afiwc/index.htm

Department of Commerce, Bureau of Export Administration http://www.bxa.doc.gov/supp4.htm

DoD, DISA Global Operations and Security Center Automated Systems Security Incident Support Team (ASSIST) http://www.assist.mil

Department of Treasury Financial Crimes Enforcement http://www.ustreas.gov/treasury/bureaus/fincen/40rec.pdf

European Union http://europa.eu.int

European Union Information Society Project Office http://www.ispo.cec.be

Federal Communications Commission (FCC) http://www.fcc.gov

Government Information Technology Services (GITS) Board http://www.gits.fed.gov

INMARSAT http://www.inmarsat.org/inmarsat/low_bankd/html/media_supp/releases/start.txt

Information Technology Resources (ITR) Board http://www.gsa.gov/irms/ka/mka/itrb

INTELSAT http://www.intelsat.int/cmc/info/intelsat.htm

InterAmerican Development Bank, http://www.iadb.org/ENGLISH/ABOUTIDB/about_idb.html

International Organization for Standardization Internet site http://www.iso.ch

International Trade Law Monitor http://itl.irv.uit.no/trade_law/documents/freetrade/wta-4/art/iia1c.html

International Telecommunication Union (ITU) http://www.itu.int

The 'Lectric Law Library ™ http://www.lectlaw.com

National Counterintelligence Center (NACIC) http://www.nacic.gov

North Atlantic Treaty Organization (NATO) http://www.nato.int/science/scope/cn.htm

Organization for Economic Cooperation and Development (OECD)
http://www.oecd.org/about/origins.htm

Organization of American States http://www.oas.org/EN/PINFO/OAS/oas.htm

Organization of American States gopher site at: gopher://oasunix1.oas.org:70/0R0-3727-pub/english/resolut/gen_assm/yr95/agd1315.txt

Sandy Bay Software, *PC Webopædia* at http://www.pcwebopaedia.com/index.html

Software Engineering Institute (SEI) http://www.sei.cmu.edu

United Nations http://www3.un.or.st/uncitral.commiss.geninfo.ht

UNESCO http://www.unesco.org/general/eng/about/index.html

United Nations Conference on Trade and Development
http://www.unicc.org/unctad/en/aboutorg/works.htm

World Bank http://www.worldbank.org/html/extdr/glance.htm

World Intellectual Property Organization http://www.wipo.int

WTO http://www.wto.org

This page intentionally left blank.

APPENDIX B

LIST OF ACRONYMS

ADP	Automated Data Processing
AECA	Arms Export Control Act
AES	Advanced Encryption Standard
AFI	Air Force Instruction
AFPD	Air Force Policy Directive
AIS	Automated Information Systems
ALECs	Alternate Local Exchange Carriers
AMIDS	Audit Monitoring and Intrusion Detection System
AO	Area of Operations
AOL	America On Line
APEC	Asia-Pacific Economic Cooperation
APII	Asia Pacific Information Infrastructure
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASEAN	Association of Southeast Asian Nations
ASSIST	Automated System Security Incident Support Team
ATD	Advanced Technology Demonstration
B,C,P,Ss	Bases, Camps, Ports and Stations
BETSI	Bellcore's Trusted Software Integrity System
BIS	Bank for International Settlements
BM/C2	Battle Management/Command and Control
BXA	Bureau of Export Administration
C&A	Certification and Accreditation
C&A WG	Certification and Accreditation Working Group
C/S/A	CINCs/Services/Agencies
C2	Command and Control
C2W	Command and Control Warfare
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAAP	Critical Asset Assurance Program
CAP	Connection Approval Program
CCL	Commerce Control List
CEC	Cooperative Engagement Capability
CERT®	Computer Emergency Response Team
CERT®/CC	CERT/Coordination Center
CFJO	Concept for Future Joint Operations
CFR	Code of Federal Regulations
CI	Counterintelligence
CIA	Central Intelligence Agency

CIAC	Computer Incident Advisory Capability
CIM	Corporate Information Management
CINC	Commander In Chief
CIO	Central Imagery Office
CIO	Chief Information Officer
CIPWG	Critical Infrastructure Protection Working Group
CIRT	Computer Incident Response Team
CISA	C4I Integration Support Activity
CITAC	Computer Investigation and Infrastructure Threat Assessment Center
CITEL	Inter-American Telecommunications Commission
CIWE	Center for Information Warfare Excellence
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joints Chiefs of Staff Instruction
CLECs	Competitive Local Exchange Carriers
CMDS	Computer Misuse Detection System
CMS	Community Management Staff
CNA	Computer Network Attack
COMSEC	Communications Security
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CSA	Computer Security Act
	Chief of Staff U.S. Army
CSAAS	Combat Support Agency Assessment System
CSPAR	CINCs Preparedness Assessment Report
DAA	Designated Approving Authority
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DBS	Direct Broadcast Satellite
DCI	Director of Central Intelligence
DDPO	Defense Dissemination Program Office
DDR&E	Director, Defense Research and Engineering
DEFCON	Defense Condition
DES	Digital Encryption Standard
DFAS	Defense Finance and Accounting Service
DG	Directorate General
	Defense Guidance
DIA	Defense Intelligence Agency
DIDS	Distributed Intrusions Detection System
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISCO	Domestic-International Satellite Consideration Order
DISN	Defense Information Systems Network
DITSCAP	DoD IT Security Certification and Accreditation Process
DMA	Defense Mapping Agency
DMC	Defense MegaCenter

DoC	Department of Commerce
DoD	Department of Defense
DoDD	Department of Defense Directive
DoE	Department of Energy
DoS	Department of State
DSB	Defense Science Board
DTAP	Defense Technology Area Plan
DTH	Direct-to-Home
EAA	Export Administration Act
EAR	Export Administration Regulation
EC/EDI	Electronic Commerce/Electronic Data Interchange
ECOSOC	Economic and Social Council
ECPA	Electronic Communications Privacy Act
EDI	Electronic Data Interchange
EFOIA	Electronic Freedom of Information Act
EOP	Executive Office of the President
EP	Electronic Protection
ETA	Education, Training and Awareness
ETAPWG	Education, Training, Awareness and Professionalization Working Group
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEDCIRC	Federal Computer Incident Response Capability
FIPS PUB	Federal Information Processing Standard Publication
FM	Field Manual
FOIA	Freedom of Information Act
FS	Federal Standard (also FED-STD)
FTS	Federal Telecommunications Service
G7	Group of Seven Nations
GAO	General Accounting Office
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GCCS	Global Command and Control System
GIE	Global Information Environment
GII	Global Information Infrastructure
GITS	Government Information Technology Services
GMITS	Guidelines for the Management of IT Security
GOSC	Global Operations and Security Center
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act
GSII	Government Services Information Infrastructure

HTML	Hypertext Markup Language
I&W	Indications and Warning
IA	Information Assurance
IAD	Information Assurance Document
IADB	Inter-American Development Bank
IAG	Information Assurance Group
IAPWG	Information Assurance Policy Working Group
IBRD	International Bank for Reconstruction and Development
IC	Intelligence Community
IC/EXCOM	Intelligence Community Executive Committee
ICSID	International Centre for Settlement of Investment Disputes
IDA	International Development Association
IEC	International Electrotechnical Commission
IEEPA	International Economic Emergency Powers Act
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFC	International Finance Corporation
ILECS	Incumbent Local Exchange Carriers
IMS	Integrated Management System
INFOSEC	Information Systems Security
INFOSYS	Information Systems
INMARSAT	International Maritime Satellite Organization
INMS	Integrated Network Management System
INTELSAT	International Telecommunications Satellite Organization
IO	Information Operations
IOC	Initial Operating Capability
IOTC	Information Operations Technical Center
IP	Internet Protocol
IPMO	INFOSEC Program Management Office
IPTF	Infrastructure Protection Task Force
IRC	INFOSEC Research Council
IRM	Information Resource Management
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITAR	International Traffic in Arms Regulations
ITMRA	Information Technology Management Reform Act
IPTF-PoA	Information Protection Task Force Plan of Action
IRT	Incident Response Team
ITR	Information Technology Resources
ITU	International Telecommunication Union
IW	Information Warfare
IW-D	Information Warfare - Defensive
IXCs	Interexchange Carriers
JCCC	Joint Communications Control Center
JIC	Joint Intelligence Center

JIT	Just-in-Time
JIWG	Joint IA Operations Working Group
JPO STC	Joint Program Office for Special Technical Countermeasures
JTF	Joint Task Force
JV2010	Joint Vision 2010
JWSTP	Joint Warfighting Science and Technology Plan
KMI	Key Management Infrastructure
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LCC	Local Control Center
LDCs	Least Developed Countries
LEA	Law Enforcement Agency
LEC	Local Exchange Carrier
LOAC	Law of Armed Conflict
MAN	Metropolitan Area Network
MARIS	Maritime Information Systems Project
MCDES	Malicious Code Detection and Eradication System
MCEB	Military Communications Electronic Board
MHz	Megahertz
MIE	Military Information Environment
MIGA	Multilateral Investment Guarantee Agency
MIT	Massachusetts Institute of Technology
MLS WG	Multilevel Security Working Group
NACC	North Atlantic Cooperation Council
NACIC	National Counterintelligence Center
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organization
NCIS	Naval Criminal Investigative Service
NCSA	National Center for Supercomputing Applications National Computer Security Association
NCSC	National Computer Security Center
NIC	National Intelligence Council
NID	Network Intrusion Detector
NIE	National Intelligence Estimate
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency
NIPRNET	Unclassified (but Sensitive) Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NITB	National INFOSEC Technical Baseline
NMCC	National Military Command Center
NRIC	Network Reliability and Interoperability Council
NRO	National Reconnaissance Office

NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSD	National Security Directive
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTIA	National Telecommunications and Information Administration
OAS	Organization of American States
OASD(C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
OCONUS	Outside the Continental United States
OECD	Organization for Economic Cooperation and Development
OEEC	Organisation for European Economic Co-operation
OET	Office of Engineering & Technology
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSE	Open Systems Environment
OSD/JS	Office of the Secretary of Defense/Joint Staff
OUSD(P)	Office of the Under Secretary of Defense (Policy)
PCC	Permanent Consultative Committees
PCCIP	President's Commission on Critical Infrastructure protection
PCS	Personal Communications Service
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKE	Public Key Encryption
POSIX	Portable Operating System for Information Exchange
PPTP	Point-to-Point Tunneling Protocol
PRA	Paperwork Reduction Act
PSYOP	Psychological Operations
QDR	Quadrennial Defense Review
R&D	Research and Development
RBOCs	Regional Bell Operating Companies
RCC	Regional Control Center
RCC PAC	RCC Pacific
RDT&E	Research, Development, Test and Evaluation
RII	Relevant Information and Intelligence
ROSC	Regional Operations and Security Center
S/A	Services/Agencies
S&T	Science and Technology

SABI WG	Secret and Below Interoperability Working Group
SAIC	Science Applications International Corporation
SATAN	Systems Administrators' Tool for Assessing Networks
SCI	Sensitive Compartmented Information
SECDEF	Secretary of Defense
SEI	Software Engineering Institute
SET	Secure Encrypted Transaction
SIO	Special Information Operations
SIPRNET	Secret Internet Protocol Routing Network
SNET	Southern New England Telephone Company
SORTS	Status of Resources and Training System
SPB	Security Policy Board
SSAA	Systems Security Authorization Agreement
TAFIM	Technical Architecture Framework for Information Management
THREATCON	Threat Condition
TRIPS	Trade-Related Aspects of Intellectual Property Rights
TRANSEC	Transmission Security
U.S.C.	U.S. Code
UCMJ	Uniform Code of Military Justice
UNCITRAL	United Nations Conference on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNISTE	UN International Symposium on Trade Efficiency
URL	Uniform Resource Locator (also Universal Resource Locator)
US	United States
USACOM	U.S. Atlantic Command
USD(P)	Undersecretary of Defense for Policy
USSS	United States Secret Service
VAS	Vulnerability Assessment System
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WEU	Western European Union
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
Y2K	Year 2000

This page intentionally left blank.

APPENDIX C

GLOSSARY

NOTE: The source of a definition is shown in brackets. Multiple definitions and their sources are shown where there is significant variance between definitions.

Access Control – Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NSTISSI 4009, 1996]

Accountability – 1. (COMSEC) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information; 2. (Information Systems) Property that allows auditing of information system activities to bet raced to persons or processes that may then be held responsible for their actions. [NSTISSI 4009, 1996]

Assurance – A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. [DODD 5200.28, 1988]

Attack – The intentional act of attempting to bypass security controls on an Automated Information System. [JIWG Proposed Common Terminology]

Attack Assessment – An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. [Joint Pub 1-02, 1994]

Authenticate – To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or other wise exposed to unauthorized modification in an information system, or to establish the validity of a transmission. [NSTISSI 4009, 1996]

Availability – Ensuring that data transmission or computing processing systems are not denied to authorized users. [CJCSI 6510.01B, 1997]

Availability of Services – Timely, reliable access to data and information services for authorized users. [NSTISSI 4009, 1996]

Banking and Finance – The retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support entities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments. [IPTF-PoA, 1996]

Clandestine Operation – An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. [Joint Pub 1-02, 1994]

Classified National Security Information – Information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [Executive Order 12958, 1995]

Client-Server Architecture – Any network-based software system that uses client software to request a specific service, and corresponding server software to provide the service from another computer on the network. [FS -1037C, 1966]

Command and Control-Protect (C2-Protect) – The maintenance of effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C2 system; C2-protect can be offensive or defensive in nature; offensive C2-protect uses the five elements of C2W to reduce the adversary's ability to conduct C2-attack; defensive C2-protect reduces friendly C2 vulnerabilities to adversary C2-attack by employment of adequate physical, electronic, and intelligence protection. [Field Manual 100-6 (adapted from CJCSI 3210.03), 1996]

Command and Control Warfare (C2W) – The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict. C2W is both offensive and defensive: a. Counter-C2 – to prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-Protection – To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influencing, degrade, or destroy the friendly C2 system. [Joint Pub 1-02, 1994] *NOTE: In Joint Pub 1-02, 1994, this definition of C2W is a replacement for Command, Control, and Communications Countermeasures.*

Commercial-off-the-shelf (COTS) – An item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Further, such items must have meaningful reliability, maintainability, and logistics historical data. [DISA, *TAFIM*, 1997]

Communications Security (COMSEC) – Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. [NSTISSI 4009, 1996]

Computer Intrusion – An incident of unauthorized access to data or an Automated Information System. [JIWG]

Confidentiality – Assurance that information is not disclosed to unauthorized entities, or processes. [NSTISSI 4009, 1996]

Continuity of Operations – The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. [Joint Pub 1.02, 1994]

Cookie – A message given to a Web browser (such as Netscape) by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When entering a Web site using cookies, a user may be asked to fill out a form providing such information as name and interests. This information is packaged into a cookie and sent to the Web browser which stores it for later use. The next time the user goes to the same Web site, the browser will send the cookie to the Web server. The server can use this information to present with custom Web pages. So, for example, instead of seeing just a generic welcome page, users might see a welcome page with their own name on it. The name cookie derives from UNIX objects called magic cookies. These are tokens that are attached to a user or program and change depending on the areas entered by the user or program. Cookies are also sometimes called persistent cookies because they typically stay in the browser for long periods of time. [*PC Webopaedia*, 1997]

Correlation – The process which associates and combines data on a single entity or subject from independent observations, in order to improve the reliability or credibility of the information. [JIWG Proposed Common Terminology]

Covert Action – An operation that is so planned and executed as to conceal the identity or permit plausible denial by the sponsor. [USC 50 § 413b]

Critical Infrastructures – Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government. [Executive Order 13010]

Cryptography – Art of science concerning the principles, means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form. [NSTISSI 4009, 1996]

Damage Assessment – 1. The determination of the effect of attacks on targets. (DoD)
2. A determination of the effect of a compromise of classified information on national security. [Joint Pub 1-02, 1994]

Damage to the National Security – Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information. [Executive Order 12958, 1995]

Data – Representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned. [Joint Pub 1-02, 1994]

Defense Information Infrastructure (DII) – The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. The DII (1) connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and (2) provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications are not considered part of the DII. [ASD(C3I) Memo, 1994]

Defensive Counterinformation – Actions protecting our military information functions from the adversary. [Air Force, *Cornerstones of Information Warfare*, 1995]

Defensive Information Operations: The defensive IO process integrates and coordinates polices and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations. Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes. [CJCSI 6510.01B, 1997]

Defense Information Systems Network (DISN) – 1. A subelement of the DII, the DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. [ASD(C3I) Memo, 1994] 2. The DISN is an information transfer network with value-added services for supporting national defense C3I decision support requirements and CIM functional business areas. As a information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services. [CJCSI 6211.02, 1993]

Denial of Service – Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. [DODD 5200.28, 1988]

Electrical Power Systems – The generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system. [IPTF-PoA, 1996]

Electronic Warfare (EW) – Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. [Joint Pub 1-02, 1994]

Emergency Services – The medical, police, fire and rescue systems and personnel that are called upon when an individual or community is responding to a public health or safety incident where speed and efficiency are necessary. [IPTF-PoA, 1996]

Event – any suspicious pre-assessed activity. [JIWG Proposed Common Terminology]

Firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. [*PC Webopaedia*, 1997]

Function – Appropriate or assigned duty, responsibility, mission, task, power, or duty of an individual, office, or organization. A functional area (e.g., personnel) comprises of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews). [Joint Pub 1-02, 1994]

Gas and Oil Production, Storage and Transportation – The holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms. [IPTF-PoA, 1996, 1996]

Global Information Infrastructure (GII) – Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services. [CJCSI 6510.01B, 1997]

Government Services Information Infrastructure (GSII) – The U.S. Government information infrastructure portion of the National Information Infrastructure (NII) used to link people to government and its services. Sometimes referred to as Government Information Technology Services (GITS). [GITS document, Chapter A-15]

Hacker – 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum

necessary [The New Hackers Dictionary, on-line]; 2. Unauthorized user who attempts or gains access to an information system. [NSTISSI No. 4009, 1996]

Identification and Authentication – Verification of the originator of a transaction, similar to the signature on a check or a Personal Identification Number (PIN) on a bank card. [CJCSI 6510.01B, 1997]

Imagery – Collectively, the representation of objects reproduced electronically or by optical means on file, electronic display devices, or other media. [Joint Pub 1-02, 1994]

Incident – An assessed event of attempted entry, unauthorized entry, and/or an information attack on a AIS. It includes unauthorized probing, browsing; disruption, or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics with or without the users knowledge, instruction or intent (e.g., malicious logic). [JIWG Proposed Common Terminology]

Indications and Warning – Those are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events. [Joint Pub 1-02, 1994]

Indicator – An action specific, generalized or theoretical, that an adversary might be expected to take in preparation for an aggressive act. [JIWG Proposed Common Terminology]

Information – 1. Facts, data, or instructions in any medium or form. [DoDD S-3600.1, 1996]; 2. The meaning that a human assigns to data by means of the known conventions used in their representation. [Joint Pub 1-02, Mar 94]; 3. Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [DISA, *TA FIM*, 1997; OMB Circ A-130, 1996]

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [DoDD S-3600.1, 1996]

Information Integrity – The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. [Executive Order 12958, 1995]

Information Security – The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [FS -1037C, 1996]

Information Superiority – That degree of dominance in the information domain which permits the conduct of operations without effective opposition. [DoDD S-3600.1, 1996]

Information System – The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organizations, and components that collect, process, store, transmit, display, and disseminate information. [DoDD S-3600.1, 1996]

Information Systems Security –The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users (includes those measures necessary to detect, document, and counter such threats). [NSTISSI 4009, 1996]

Information Warfare (IW) – Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. [DoDD S-3600.1, 1996]

Infrastructure – The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of governments at all levels, and to society as a whole. [CIWG, *Report: Options*]

Infrastructure Assurance – The surety of readiness, reliability, and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities. [CIWG, *Report: Options*]

Integrity – Absolute verification that data has not been modified in transmission or during computer processing. [CJCSI 6510.01B, 1997]

Intelligence Estimate – The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. [Joint Pub 1-02, 1994]

Interoperability – The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. [Joint Pub 1-02, 1994]

Java – A high-level, object-oriented programming language similar to C++, but simplified to eliminate language features that cause common programming errors. Java source code files (files with a .java extension) are compiled into a format called bytecode (files with a .class extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as Java Virtual Machines

(VMs), exist for most operating systems, including UNIX, the Macintosh OS, and Windows. Bytecode can also be converted directly into machine language instructions by a just-in-time compiler (JIT). Small Java applications, called Java applets, can be downloaded from a Web server and run on a computer by a Java-compatible Web browser, such as Netscape Navigator or Microsoft Internet Explorer. Microsoft has stated that it intends to include a Java interpreter in future versions of Windows, which will enable users to execute Java applets directly from the operating system. [*PC Webopaedia*, 1997]

Legacy Systems – Systems that are candidates for phase-out, upgrade, or replacement. Generally, legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out (eliminated). Such systems may or may not operate in a legacy environment. [TAFIM, 1997]

Local Area Network (LAN) – A data communications system that lies within a limited spatial area, has a specific user group, has a specific topology, and is not a public switched tele-communications network, but may be connected to one. (Note: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN). LANs are not subject to public telecommunications regulations. [FS -1037C, 1996]

Malicious Logic – Hardware, software, or firmware that is intentionally included into an information system for an unauthorized purpose (e.g., virus & Trojan horse). [JIWG Proposed Common Terminology]

Middleware – Software that connects two otherwise separate applications. For example, there are a number of middleware products that link a database system to a Web server. This allows users to request data from the database using forms displayed on a Web browser, and it enables the Web server to return dynamic Web pages based on the user's requests and profile. The term middleware is used to describe separate products that serve as the glue between two applications. It is, therefore, distinct from import and export features that may be built into one of the applications. Middleware is sometimes called plumbing because it connects two sides of an application and passes data between them. In a three-tier architecture, middleware occupies the middle tier. [*PC Webopaedia*, 1997]

National Information Infrastructure (NII) – 1. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. [Joint Pub 3-13, Draft, 1997]. 2. System of high-speed telecommunications networks, databases, and advanced

computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits. [IITF, *NII Security: The Federal Role*, 1995]

National Security Systems – Those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involve intelligence activities, involve cryptologic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the direct fulfillment of military or intelligence missions. [NSD-42, 1990]

Nonrepudiation – Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data. Digital signatures are the current non-repudiation technique of choice for the NII. [NSTISSI 4009, 1996; Joint Pub 1-02, 1994]

Offensive Information Operations – The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. [Joint Pub 3-13, Draft, Jul 1997]

Open Network Architecture – A regulatory framework imposed by the FCC on communications carriers (the long distance telephone carriers such as AT&T and the Regional Bell Operating Companies) which requires the carriers to provide competing service providers with access to basic communications services on an equal basis. [NIST Special Pub 800-11, 1995]

Open System – 1. A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (a) to be ported with minimal changes across a wide range of systems, (b) to interoperate with other applications on local and remote systems, and (c) to interact with users in a style that facilitates user portability. [PCCIP]; 2. A system with characteristics that comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards. [FS -1037C, 1996]

Open Systems Environment (OSE) – The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. [TAFIM, 1997]

Operations Security (OPSEC) – OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems, (b) Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [Joint Pub 1-02, 1994]

POSIX – Acronym for portable operating system interface for computer environments. A Federal Information Processing Standard Publication (FIPS PUB 151-1) for a vendor-independent interface between an operating system and an application program, including operating system interfaces and source code functions. IEEE Standard 1003.1-1988 was adopted by reference and published as FIPS PUB 151-1. [FS -1037C, 1966]

Precedence –A designation assigned to a message by the originator to indicate to communications personnel the relative order of handling and to the addressee the order in which the message is to be noted. [Joint Pub 1-02, 1994]

Protocol – 1. Set of rules and formats, semantic and syntactic, that permits entities to exchange information. [NSTISSI 4009, 1996]; 2. A formal set of conventions governing the format and control of interaction among communicating functional units. Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communications over a data link are performed in terms of the particular transmission mode, control procedures, and recovery procedures. In layered communications system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy. [FS -1037C, 1996]

Psychological Operations (PSYOP) – Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (PSYOP are a vital part of the broad range of U.S. political, military, economic, and informational activities. When properly employed, PSYOP can lower the morale and reduce the efficiency of enemy forces and could create dissidence and disaffection within their ranks.) [Joint Pub 3-53, 1993]

Risk – The probability that a particular threat will exploit a particular vulnerability of the system. [NSA, NCSC *Glossary*, 1988]

Risk Analysis – The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. [NSA, NCSC *Glossary*, 1988]

Risk Assessment – Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on

national security and using the analysis as a basis for identifying appropriate and cost-effective counter-measures. Synonymous with risk analysis. [NSTISSI No. 4009, 1996]

Risk Management – The total process of identifying, measurement, controlling, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. [NSTISSI No. 4009, 1996]

Sensitive Information – Information, the loss, misuse, or unauthorized access to modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or and Act of Congress to be kept secret in the interest of the national defense or foreign policy. Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). [NSTISSI No. 4009, 1996]

Social engineering – A deception technique utilized by hackers to derive information or data about a particular system or operation. [PCCIP, *Hacker Primer*, 1997]

Tactical Warning – 1. A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. 2. In satellite and missile surveillance, a notification to operational command centers that a specific threat event is occurring. The component elements that describe threat events are: (a) country of origin – country or countries initiating hostilities, (b) event type and size – identification of the type of event and determination of the size and number of weapons, (c) country under attack – determined by observing trajectory of an object and predicting impact point, and (d) event time – time the hostile event occurred. [Joint Pub 1-02, 1994]

Technical Attack – Attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, rather than by subverting system personnel or other users. [NSTISSI 4009, 1992]

Telecommunications – 1. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electro-mechanical, electro-optical, or electronic means. [NSTISSI 4009, 1996]; 2. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. [Joint Pub 1-02, 1994]

Threat – Any circumstance or event with the potential to cause harm to an AIS in the form of destruction, disclosure, modification of data, or denial of service. [JIWG Proposed Common Terminology]

Transmission Security (TRANSEC) – Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. [NSTISSI 4009, 1996]

Transportation – The aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from a point-of-origin to a destination point in order to support and complete matters of commerce, government operations, and personal affairs. [IPTF-PoA, 1996]

Trashing – Hacker term for physically entering the trash containers at a target site in hopes of finding valuable information such as passwords, system documentation, or employee personal information to be used for social engineering attacks. [PCCIP, *Hacker Primer*, 1997]

Virtual Network – 1. A network that provides virtual circuits and that is established by using the facilities of a real network [FS -1037C, 1996]; 2. A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable one to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. [*PC Webopaedia*, 1997]

Virus – Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [NSTISSI 4009, 1996]

Water Supply Systems – The sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration and cleaning systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with waste water and fire fighting. [IPTF-PoA, 1996]

Web Server – A computer that delivers (serves up) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL, http://www.sandybay.com/index.html, in your browser, this sends a request to the server whose domain name is sandybay.com. The server then fetches the page named index.html and sends it to your browser. Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications, including public domain software from NCSA and commercial packages from Microsoft, Netscape and others. [*PC Webopaedia*, 1997]

F

G

H

I

J

K

L

M

N

O

P

Q

R

S